Cyberstalking, electronic eavesdropping, and other online shenanigans

Alberta Family Law Institute: Survive, Strive, Thrive

Calgary 2024

Cody P. Stokowski

Stokes Law (Calgary)

1. Introduction

- Development of our digital presence.
- Technological advancements and their impact on child safety.
- The importance of safeguarding children's digital footprints.
- Practical Considerations to safeguard children.

2. Allowing Children to Use Social Media and Parental Monitoring Apps

- **2.1 Statistics on Parents Supervising and Limiting the Sharing of Personal Information Online by a Child**
- **2.2 The Role of Parental Monitoring Apps**
    - Overview of apps designed for parental control (e.g., mSpy, Eyezy).
    - Balancing privacy and safety: How monitoring apps can be used responsibly.
    - To control and monitor or not: How to openly discuss monitoring

3. Sharenting and Social Media: Sharing Children's Photos Online by Parents

- **3.1 The Rise of Sharenting**
    - Defining “sharenting” and its popularity among parents.
    - Legal risks and privacy concerns associated with sharing children’s photos online.
    - Public campaigns like Deutsche Telekom's #ShareWithCare: Raising awareness about responsible sharenting.
    - Practical Considerations.

4. Family Violence and Cyberstalking: Protecting Children and Families Online

- **4.1 Cyberstalking, Hacking, and Family Violence**
    - How digital environments facilitate new forms of family violence.
    - Examples of cyberstalking behaviors, such as hacking accounts and accessing private information.
- **4.2 Disconnecting and Restricting Access: Legal and Technical Measures**
    - Steps for protecting digital accounts

5. Tracking Internet Usage, Location Monitoring and Managing Location Services

- **5.1 Types of Trackers**

    - Overview of trackers (e.g., Apple AirTags, Samsung SmartTags, Tile).
- **5.2 Safety Measures: Detecting and Disabling Trackers and Managing Location Services**
    - Instructions for detecting and disabling trackers on various devices (e.g., Android 14's manual search, iOS 16's Safety Check feature).
    - Use of applications such as Tracker Detect and AirGuard for detecting Bluetooth trackers.
- **5.3 Monitoring Tool Abuse**
- **5.4 Legal Implications of Unauthorized Tracking**
    - Criminal liability for unauthorized use of tracking devices.

6. Law Firm Cyber Protection

- How to protect your firm from cyber security threats.

1. Introduction

"*Get with the times, Mom and Dad*."

A common phrase that we take for granted as we age, and new technology and fashions emerge which surpass our knowledge. But now, more than ever, we should be concerned about the implications of not staying up to date with new technology and the safety risk children face because of our careless oversight and oversharing of their information.

The purpose of this paper is to explore how technology is impacting the safety of our family law clients, and their children. We will explore the importance of advising our clients on how to safeguard the digital identities of their children, as well as themselves.

As we will explore in this paper, technological advances in artificial intelligence ("AI") put our children at risk of having their identity stolen, and their image used by bad actors for personal benefit or enjoyment. The example used in the conference will be a campaign coined "#ShareWithCare" created by Deutsche Telekom, which involves an exaggerated narrative of a 9-year-old girl who is AI-aged with deepfake technology to age her and allow her to confront her parents about the consequences of her image and information being shared online.[1]

In addition to providing an overview of some resources, when used with good intentions, that parents can use to monitor their children's activity on smartphones, we will also see how such resources can be abused between separated parents.

Technology can be used for good or for bad. I have done my best to expose you to both the good and the bad so that you may be better informed about the risks our clients and their children face if used incorrectly.

Development of our digital presence

February 2004[2]…February 2005[3]…October 2010[4]…Three dates that to many have no real meaning; however, what we are looking at are the birth dates of three of the most significant online social media platforms: Meta (formerly Facebook), Youtube, and Instagram (and many less prevalent applications in between, such as Whatsapp, Snapchat, and X (formerly Twitter). In retrospect, the time that has lapsed since 2004 seems notional; however, in these 20 or so years there have been quantum leaps in technology including the development of AI and digital

---

1 Detsche Telekom, "Sharenting" (Jul 13, 2023), online (video): <https://youtu.be/FrdhsX8R_AY?si=w1V5aXl0vDzfT3py>.

2 Meta (formerly Facebook) was founded.

3 Youtube was created by Google.

4 Instagram was founded.

currencies on blockchains[5]. With the founding of these platforms came about new concerns about how our information is shared and the size of our personal "digital footprint.[6]"

One of the primary concerns of increasing access to our personal information is identity theft. In 2014, approximately six (6) out of every 100,000 Canadian residents were affected by identity theft.[7] In 2023, that number has doubled to approximately 13. These statistics are consistent with a recent release by the Canadian Competition Bureau which shows that in the past ten years, fraud cases in Canada have increase from 79,000 to 150,000 between 2012 and 2022.[8] What can we as Canadians, lawyers, and parents, be doing better at to prevent these numbers from doubling again in the next ten years? The answer is, better safeguarding our digital footprint and that of our dependent children.

Many of us currently practicing in the legal profession had our first exposure to these social media platforms well into our teen or young adult years. Some others have never been able to keep up with the never-ending updates in the applications themselves and have already fallen behind. And despite the minimal digital footprint that many of us have predating 2004, we are still susceptible to identity fraud. Now, think about the many young adults who have been developing their digital footprint on social media since they were nothing more than an ultrasound photo and a tagged location on Meta/Facebook thanks to their parents. Think about how large their digital footprints are relative to ours. Since the time their ultrasound photo was posted up harmlessly, we can trace the date and location of their birth, the primary schools they attended, the university they graduated from, the company they have surrounded themselves with, the employers they have had, their religion and sexual orientation, and where they have set down roots. Many social media accounts are an online passport to an individual and their life. Many parents treat their Instagram accounts as digital photo albums to be shared with not only family and close friends, but many strangers who they have never met in real life. This is referred to as "oversharenting.[9]"

---

5 Such as Etherum and Bitcoin.

6 For definition see IBM, "What is a digital footprint?", online <https://www.ibm.com/topics/digital-footprint>.

7 Statista, "Rate of identity thefts in Canada from 2012 to 2023" (July 2024), online, <https://www.statista.com/statistics/544904/identity-theft-rate-canada/>.

8 Competition Bureau Canada – Government of Canada, "the rise of AI: Fraud in the digital age" (Mar 4, 2024), online <https://www.canada.ca/en/competition-bureau/news/2024/03/the-rise-of-ai-fraud-in-the-digital-age.html>.

9 CBC, Amy Bell, "Oversharenting: Are you giving away too much about your kids online?" (Apr 24, 2019), online <https://www.cbc.ca/news/canada/british-columbia/parenting-online-social-media-oversharenting-1.5107340>.

Technological advancements and their impact on child safety

If it wasn't enough that an individual's entire life journey is now online for everyone to access, AI has now provided fraudsters with the ability to impersonate other individuals. They are able to generate convincing fake communications with voice cloning and utilize deep-fake[10] technology to impersonate or replicate another's facial image when communicating online.[11]

The importance of safeguarding children's digital footprints

Deepfake technology has been used to make "entertaining and satirical content[12]" which many have enjoyed. For example, the endless videos of Tom Cruise's face being imposed over that of Youtube influencers using AI technology.[13] Although this seems harmless, there have been cases where such technology is causing safety concerns for people and their children. For example, online content with the help of AI deepfake has gone so far as to include placing celebrity photos over pornographic photos and videos…but more concerning is the inclusion of our children's images in pornographic materials. Our children didn't consent to their photos being shared on social media. Nor did they share the photos themselves. We are their parents who spoon-fed their images to bad actors.

Our job is to ensure there are safeguards implemented to limit their exposure to risk to the extent it can be. We must be able to adapt and think forward. Inherently, concerns with the misuse of a child's digital footprint will only grow with the emergence of technological advances. We need to contemplate whether images of children will be shared electronically online, and if so, how and to what extent. As we will explore in this paper, there needs to be an increase in the awareness of responsible online sharing of our children's information and development of their digital footprint.

We need to start working with our clients to contemplate a child's smart device usage, the parental controls that govern their devices, the applications they have access to, restricting the information children are allowed to share, and the social media accounts they have permission to maintain (if any).

At first blush, perhaps the best thing to do is simply monitor their smart devices. Or perhaps it's not to let them use one at all until a specific age. This is really a social question that parents need

---

10 Business Insider, Dave Johnson and Alexander Johnson, "What are deepfakes? How fake AI-powered audio and video warps our perception of reality" (Jul 25, 2023), online <https://www.businessinsider.com/guides/tech/what-is-deepfake>.

11 Canadian Security Intelligence Service – Government of Canada, "Deepfakes: A Real Threat to a Canadian Future" (Nov 16, 2023), online <https://www.canada.ca/en/security-intelligence-service/corporate/publications/the-evolution-of-disinformation-a-deepfake-future/deepfakes-a-real-threat-to-a-canadian-future.html>.

12 *Ibid.*

13 Vecanoi, "Very realistic Tom Cruise Deepfake / AI Tom Cruise (Feb 28, 2021), online (video) <https://youtu.be/iyiOVUbsPcM?si=TvIYFqM6WPNHJHLy>.

to become better informed to determine what is in their child's best interest. Currently, there is minimal "law" around what is appropriate usage and age for children. Only quasi-legislative law such as bylaws or policies in educational institutions limit device usage or access to smart devices. It's our job as family lawyers to develop the decision-making and parenting terms that will be in the best interests of these children and safeguard their digital footprints.

Practical Considerations to safeguard children

How do we as legal counsel ensure that we are effectively advising our clients with children about the importance of safeguarding their child's digital footprint? How do we structure terms around how a child's photos, life milestones, and information are shared? How do we structure terms that compel the parents to limit the child's sharing of information online. To what extent should parents have the ability to decide what is in their child's best interests with respect to their online presence? Should parents be at liberty to install applications on their child's smart device which monitor and control the child's social media activity? Within this paper, we explore some of these thoughts and provide some helpful resources to counsel.

2. Allowing Children to Use Social Media and Parental Monitoring Apps

In today's connected world, social media is a big part of children's lives, offering both fun interactive opportunities and some serious challenges for parents. While platforms like Instagram and TikTok can spark creativity and help kids connect with friends, they can also expose them to risks like identity theft, safety risks, and inappropriate content. That's why many parents are turning to parental monitoring apps to keep an eye on their kids' online activities. These apps help parents set rules, track interactions, and encourage safe online habits, all while promoting conversations about being responsible in the digital world. Striking the right balance between allowing our children to enjoy social media, and providing them with some level of privacy, is important.

As we will see from statistics, there are many parents who need to become better informed about how they themselves should share information online, as well as being better informed about supervising their children's online activity and information sharing.

2.1 Statistics on Parents Supervising and Limiting the Sharing of Personal Information Online by a Child

It has been cited[14]:

- 86% of children use the internet.
- 95% of the parents of these children would not allow their children to submit their photographs to an internet site.
- 76% of parents report they check bookmarks or browser history of their child's device, while 16% use monitoring software.
- 17% of parents minimally supervise or monitor their child's internet/online usage.
- 29% of parents have rules regarding their child's usage of the Internet and avoidance of specific sites. However, 30% have no set rules at all.

30% of parents have no rules on how their children interact online or use the internet and 17% minimally supervise their children. Why is this a concern? Four children – between the ages of eight and 12 years of age – were found to have shared intimate images or videos of themselves online.[15] At this age, no one is limiting when or how these children could use a device and the internet. No one is protecting their digital footprint. Once these images are online, it may be impossible to remove them or their metadata.

2.2 The Role of Parental Monitoring Apps

Overview of apps designed for parental control

Parental monitoring apps exist for parents to install on their child's device (generally in stealth mode whereby the app is hidden on the device from the child's view), allowing them to monitor their child's online activities, including social media, text messaging, web browsing, and calls (ongoing and history). Many of the popular social media platforms, such as Meta/Facebook, Instagram, WhatsApp, and Snapchat, can be monitored. Some applications allow parents to view deleted messages and monitor their direct messages from online users. Others monitor the smart devices text messages, iMessages, and have a keylogger feature which captures all typed content for parents to know their child's passwords and frequent phrases.

Examples of prevalent parental monitoring applications are:

---

14 Media Awareness Network, "Canada's Children in a Wired World: The Parent's View", online <https://mediasmarts.ca/sites/default/files/pdfs/publication-report/full/YCWWI-parents-view.pdf>.

15 Global News, Callum Smith, "Monitoring child's online activity is parental responsibility: RCMP" (Jan 3, 2019), online <https://globalnews.ca/news/4812608/monitoring-childs-online-activity/>.

1. mSpy[16]: Incognito social media app and message viewing, screenrecorder to regularly record screen activity with screenshots, keylogger, web browsing history, remote access to call logs, view media like photos and videos, and GPS tracking.
2. Eyezy[17]: Incognito social media app and message viewing, AI software to monitor activity and alert of wrongdoings, keylogger, web browsing history, remote access to call logs, and view media like photos and videos.
3. Aura[18]: Parental control software to filter, block and monitor applications, dark web usage, pause internet, and safer online gaming.

Balancing privacy and safety: How monitoring apps can be used responsibly

The benefits of these types of applications are that parents are able to see flagged, inappropriate content, stop inappropriate sharing of content by their children, and to quickly identify if their child is being groomed online by a bad actor.

These apps also assist with monitoring screen time and help with blocking specific applications that the child should not be accessing.

It is important for us as legal counsel to be contemplating and recommending whether either parent, or both parents, or neither parent, should have access to those monitoring features outlined above.

Although the above may be in the child's best interests, as we will discuss within this paper, there are opportunities for these applications to be abused by a parent and for ulterior motives such as tracking the other party and their online activity.

What if there are allegations of family violence, specifically between the child and one of the parents? What if the child depends on their mobile device to text one of their parents about concerns while in the care of the other? Do such applications otherwise hamper telephone / communication between a parent and their child?

To control and monitor usage or not: How to openly discuss monitoring

A criticism of utilizing a parental monitoring app includes the different perspective by parents and their child. A child may wish to negotiate exemptions to rules around their usage and information sharing, and have a certain level of privacy. Parents may wish to have an all-or-nothing approach with complete unhampered access to all information available on the child's smart device. One of

16 https://mspy.net
17 https://www.eyezy.com/
18 https://www.aura.com/parental-controls

the negative responses by a child is the lack of consultation and understanding as to the imposition of the application.[19]

Parents may wish to work with a family counsellor to better explain the risks children face with online use, and why specific clauses have been agreed upon between co-parents to protect them.

Useful clauses for orders may include:

> *Neither party shall monitor the Child(ren) through a third-party parental monitoring application.*
>
> *The __[party]__ shall not monitor the Child(ren) through a third-party parental monitoring application.*
>
> *The smart device shall have parental monitoring software installed, accessible by both parents, to track screen time, location, and usage.*
>
> *Both parties shall have access to the log in credentials to the parental monitoring application ___[app name]__ for the specific purposes of monitoring the Child(ren)'s social media messaging, text messaging, iMessaging, WhatsApp usage, social media usage, screen usage, keylogger, web browsing history, call logs, block and monitor applications, restrict communication with [specific individual], view media including photos and videos, and GPS tracking.*
>
> *The parties shall, during their parenting time, ensure the Child(ren) does not post personal information online or on any social media platforms, including but not limited to: selfies, personal address, personal activity schedules, location, personal email address, or date of birth.*
>
> *The parties shall supervise any and all internet usage by the Child(ren) during their parenting time.*
>
> *Neither party shall provide the Child(ren) with a smartphone or smartwatch until the Child(ren) reach(es) the age of __[age]__.*
>
> *Neither party shall allow the Child(ren) to register or enroll with Facebook/Instagram/X/WhatsApp/TikTok/Snapchat until the Child(ren) reach(es) the age of __[age]__.*
>
> *Both parties shall ensure the Child(ren) does not have possession and/or control over a computer, smartphone, or smartwatch in their bedroom at any time.*

---

19 Boston Children's Digital Wellness Lab, "Safety and Surveillance Software Practices as a Parent in the Digital World", (Nov 2023), online <https://digitalwellnesslab.org/research-briefs/safety-and-surveillance-software-practices-as-a-parent-in-the-digital-world/>.

Both parties shall ensure the Child(ren) has access to their smartphone from _[time]_ to _[time]_ while in the care of the other party, and ensure the device remains charged at all times.

Either party may elect to turn off the Child(ren)'s smart device(s) at _[time]__ each day during their parenting time.

Smart device use by the Child(ren) shall be restricted to ___[time limit]__ per day.

The Child(ren) shall be restricted to accessing the internet to a maximum of ___[time limit]__ per day.

Neither party shall allow the Child(ren) to install new apps or games on the smart device without prior written consent from the other party.

The smart device must be configured with restrictions on content and usage, including age-appropriate settings, screen time limits, and app approval controls.

3. Sharenting and Social Media: Sharing Children's Photos Online By Parents

3.1 The Rise of Sharenting

Defining "sharenting" and its popularity among parents

"Sharenting" is a relatively new term coined in 2012 (yet new to many) representing the act of over sharing a child's image and life milestones online.

It is defined as the "The action or practice of sharing news, images, or videos of one's children on social media websites.[20]"

Recent studies have found[21] :

- 75% of parents have posted content about their children online. 74.4% of the content are photos and/or videos of the child.
- 41% of parents share "everyday life" of their children.
- 27% of parents are anxious about discussing sharenting, while 51% were interest and wanted to learn more about it and the risks.

---

20 Oxford University Press, "Sharenting" (2022), online <https://www.oed.com/dictionary/sharenting_n>.

21 National Library of Medicine, "Sharenting; characteristics and awareness of parents publishing sensitive content of their children on online platforms", (Jul 30, 2024), online <https://pmc.ncbi.nlm.nih.gov/articles/PMC11290302/#:~:text=Among%20parents%20using%20one%20or,their%20children%20on%20social%20media>.

Another study found[22]:

- 84% of mothers with children under the age of two had posted images of those children online; and
- The average child appears in about 195 shared photographs each year (approximately 1,000 images in the first five (5) years).

It is estimated that by 2030, two-thirds of all identity theft cases will involve sharing.[23]

Legal risks and privacy concerns associated with sharing children's photos online

Based on the above statistics there can be a desire for parents to share their children's achievements as a means of being proud and showing support, but unknowingly also sharing pertinent personal information of the child. While sharing photos online, parents often forget the metadata (including location) built into a photo and post online. They also fail to limit permissions to strangers and restrict the use and control of their child's images that they share or upload to a website.

Parents are neglecting to understand that every time they post those images, blogs, or personal information, they increase their child's digital footprint. This oversight while over-sharing by a parent, can put the child at risk of identity-theft.

Public campaigns like Deutsche Telekom's #ShareWithCare: Raising awareness about responsible sharenting

Emerging new technology such as advances in AI, put our children at risk of having their identity stolen, and their image used by bad actors for personal benefit or enjoyment. The example used at the conference will be a campaign coined "#ShareWithCare" created by Deutsche Telekom[24]. The video involves an exaggerated narrative of a 9-year-old girl, who had their image AI-aged with

---

22 Commissioner for Children & Young People, "Sharenting" (2018), online <https://www.ccyp.com.au/wp-content/uploads/2019/02/CCYP_2018.3.13_sharenting_infographic_final.pdf>.

23 Telekom, "ShareWithCare: Telekom raises awareness for responsible use of children's photos on the Internet" (Jul 3, 2023), online <https://www.telekom.com/en/company/details/share-with-care-telekom-raises-awareness-1041810>.

24 *Ibid.*

deepfake technology without her consent, to age her and allow her to confront her parents about the consequences of her image and information being shared online.[25]

The video brings awareness to parents about the importance of responsibly sharing information about their child, and how AI technology is being used to commit identity theft. As we saw, Ella has had voice cloning and AI deep-fake aging applied to her to create an aged identity.

As alluded to at the outset of this paper, one of the most important considerations with deepfake AI aging of child photos is child abuse / pornographic imagery. It may involve realistic but simulated abuse situations whereby images of adults resembling minors or aging children to be older. These children didn't consent to their photos being shared on social media. Nor did they share the photos themselves. We are their parents who spoon-fed their images to bad actors. The negative effects cannot be overstated.

The recent decision by the Honourable Justice C.L. Daniel in the Alberta Court of Justice decision of *R v Prys,* 2024 ABCJ 166 stated the following as it relates to the distribution of child pornography and its effects:

> ***HARM IDENTIFIED IN CHILD PORNOGRAPHY CASES***
>
> *[15] It is now understood that pornography involving real children is an aggravated form of child sexual abuse, with never-ending victimization. Once a photo or movie is distributed on the internet, the moment of that child's utmost degradation is permanently public. Further, it is now evident that child pornography distorts the thought process of its consumers, making child abuse seem normal and justifiable. Child pornography may be used to groom child victims, but it also has the effect of grooming offenders. The ever-increasing market for child pornography thus creates more victims.*
>
> *[16] The* ***R v Jonat****, 2019 ONSC 1633 case, discusses the true nature of the evil of child pornography, and the fallacy of viewing such offences as being passive in nature without direct victim impact. At paras 26-29, the Court observes:*
>
> > *[26] In a pre-internet world, the ability of people inclined towards pedophilia to find like-minded individuals, share experiences, cultivate their fantasies and seek access to victims was naturally constrained by the isolation imposed by their relatively small numbers and by the very great fear of the consequences of discovery.*
> >
> > *[27] Modern technology has considerably blunted both restraints. The internet has largely defeated the former isolation of pedophiles. Once scattered individuals are now able to find each other. In doing so, they acquire the strength and far greater potential for harm of what amounts to nothing less than a virtual support*

---

[25] *Supra note* 1.

group from a world-wide community unified by shared illicit interests in the exploitation of children. It has also blunted their fear of discovery by cloaking their activities in the apparent anonymity of the internet and the potential complexity of cross-border law enforcement.

[28] The result has been a virtual firehose of pornographic images of victimized children spewed across the internet. These images are collected and added to by participants, spawning imitators in their thousands. Chat groups and peer-to-peer platforms proliferate by which pedophiles encourage each other either to violate children to whom they have access or to encourage others to do so and share pictures of their exploits. A veritable barter economy has grown around the collecting of these pictures and videos. There are numerous instances of such trading to be found in relation to Mr. Jonat's on-line activities. The currency of trade in this "economy" is not money but the possession of tradable pornographic material – the fresher and the more extreme the better. In this fashion barriers constraining the once isolated individual from progressing from voyeur to active perpetrator are eroded and the numbers of harmed children grows exponentially.

[29] Once images or videos are circulated, the degradation of these children becomes both permanent and global. Images once distributed through this informal network can never be truly eliminated from circulation. The harm is both acute and perpetual. The growing numbers of victims – most unidentified - suffer from wounds that are continually re-opened and harm that can manifest itself over decades.

...

[24] Society is now well-aware that live sexual abuse against children is recorded on media, and then sold and circulated on the Internet. Victims are then powerless to stop others from accessing, possessing or sharing the material that depicts their abuse. Although victims may not be readily identifiable, their anonymity does not reduce the harm they experience. The Internet has fostered and accelerated the proliferation of child pornography. With the ease of instantly distributing these materials globally, victims face the reality that anyone they meet, anywhere in the world, has potentially witnessed, and derived sexual gratification from their sexual abuse. Many go on to accept continuing physical sexual abuse as their lot in life.

Practical Considerations

Prior to parents deciding whether images of their children will be shared electronically online, and if so, how and to what extent, we should promote parents to become better informed and aware of the implications and risks of them oversharing their children's photos, news, and information. A great resource is available at teachtoday.de/en/[26]

The Honourable Justice N.W. D'Souza of the Alberta Court of Justice in *Gordon v Broan*, 2018 ABPC 44, directed the following clause which provides some helpful guidance on the phrasing to resolve these issues:

> *Both parties shall not post or disseminate inappropriate photographs or images of themselves and/or the child on any form of social media to include Instagram, Meta/Facebook and the like.*

Additional clauses may include the following:

> *The __[party]__ who shared the photos of the Child shall immediately have them removed from any online website or platform and from any other electronic form of application, software, database, social media platform, or communication method.*
>
> *Neither party shall post, share, or disseminate images of the Child(ren) on any form of social media platform to include Instagram, Meta/Facebook, X, and the like.*
>
> *The __[party]__ shall make all reasonable efforts to ensure that their new partner does not post, share, or disseminate images of the Child(ren) on any form of social media platform to include Instagram, Meta/Facebook, X, and the like.*
>
> *Neither parent shall permit third parties, including new partners, family members, or friends, to share any personal information or images of the Child(ren) on social media platforms unless explicitly agreed upon in writing by both parents.*
>
> *The parties shall not share or post the Child(ren)'s location, address, school, date of birth, images of documentation, or the like online.*
>
> *Any photos posted online by either party which include the Child(ren) shall have their faces redacted, blurred, or otherwise censored.*
>
> *The parties shall only share photos and personal information pertaining to the Child(ren) through Our Family Wizard.*
>
> *Neither party shall tag or link the Child(ren) in any social media posts.*

[26] Telekom, "TeachToday", online <https://www.teachtoday.de/en/>.

Neither parent shall create, maintain, or authorize any account, profile, or digital footprint in the Child(ren)'s name or on their behalf on any social media platform without written consent from the other parent.

If either parent intends to share any information about the Child(ren) that may indirectly disclose personal details they must obtain prior written consent from the other parent.

4. Family Violence and Cyberstalking: Protecting Children and Families Online

4.1 Cyberstalking, Hacking, and Family Violence

Cyberstalking is generally defined to include the "use of digital technology to track and harass someone."[27]

In 2014, approximately 2.5 Canadians experienced cyberstalking within the previous five (5) years.[28]

How digital environments facilitate new forms of family violence

It has been cited as a tech-based form of abuse that falls within the definition of domestic and family violence and coercive control in Australia.[29]

As we will explore within this paper, cyberstalking doesn't only include being stalked on social media or through a dating app, it can also include GPS tracking technologies built into different smart device apps, the use of a Bluetooth tracking device, hidden cameras, audio bugs, spyware, reverse image searches, and online maps / post location metadata.

---

27 eSafety Commissioner - Australian Government, "Cyberstalking", online <https://www.esafety.gov.au/key-topics/staying-safe/cyberstalking>.

28 Statistics Canada – Government of Canada, "Women and men who experienced cyberstalking in Canada" (Jun 5, 2018), online <https://www150.statcan.gc.ca/n1/pub/75-006-x/2018001/article/54973-eng.htm>.

29 *Supra note* 27.

Examples of cyberstalking behaviors, such as hacking accounts and accessing private information

People who cyberstalk may use a range of online and offline technologies including email stalking, internet stalking, and computer stalking[30]:

- global positioning system (GPS) trackers;
- keyloggers;
- hidden cameras or webcams;
- audio bugs, microphones, telephones;
- location-based dating apps;
- spyware, mobile stalker apps;
- email accounts;
- social media;
- online maps;
- reverse image searches;
- 'find my device' services; and
- Bluetooth trackers as explained herein.

Examples of cyberstalking behaviours include[31]:

- sending or posting offensive online messages, images or personal information;
- tracking online activity or location;
- stealing or intercepting online information;
- blackmail;
- doxing;
- destroying or manipulating data;
- impersonating someone online; and
- following, monitoring or tracking a person's location and activities.

30 Victorian Klaw Reform Commission, "Stalking: Final Report – Responses to cyberstalking" (Oct 28, 2022), online <https://www.lawreform.vic.gov.au/publication/stalking-final-report/3-responses-to-cyberstalking/>.

31 Norton, "Cyberstalking: What it is and how to protect yourself" (Feb 28, 2024), online <https://us.norton.com/blog/how-to/what-is-cyberstalking>.

4.2 Disconnecting and Restricting Access: Legal and Technical Measures

Steps for protecting digital accounts

Your client should take proactive steps to disconnect and restrict any unauthorized access of their ex-spouse/partner from access to their digital accounts. If not done, it is possible that their location can be tracked, their conduct and activity can be traced including future plans, privileged or confidential information may leak to the other party, and they may be abused by environmental changes (referred to as small gaslighting).

A non-exhaustive checklist to provide your clients is as follows[32]:

- Change passwords for email, banking, social media, and other applications such as home tech apps, media accounts, ride share apps, and food delivery apps;
- Enable multi-factor authentication in settings on all devices;
- Turn location services off (see next topic);
- Ensure their social media accounts are turned to "private" and they have unfriended their ex;
- Remove and Apple ID device linking (see Apple ID settings and "Find my" app setting);
- Determine where information is backed up and remove access to those folders / platforms – Dropbox, Google, Amazon, OneDrive, etc.
- Delete all unknown apps off of their smart devices;
- Change email address;
- Change phone number;
- Encrypt data on their laptop and external hard drives;
- Remove access to any joint mobile phone or internet plans;
- Remove access to any joint bank or credit accounts;
- Delete stored passwords in any Keychain / Password Managers;
- Monitor for unusual activity or data usage;
- Revoke access to social media accounts;
- Turn off Bluetooth;
- Remove geo-tags from social media photos;
- Ensure the Ring Doorbell account or any other smart home devices are not accessible by the other party; and
- Log out of all devices on Apple, Google Account, Netflix, Disney+, Amazon Prime, or otherwise.

---

[32] Clinic to End Tech Abuse, "Resources", online <https://ceta.tech.cornell.edu/resources>.

Additional free resources, including safety guides for Android, Google (and Gmail), iCloud and Hotmail can be found at the Clinic To End Tech Abuse at https://ceta.tech.cornell.edu/resources.

5. Tracking Internet Usage, Location Monitoring and Managing Location Services

Bluetooth devices have become increasingly popular to track the whereabouts of our personal belongings such as keys, wallets, phones, bags, luggage, and bicycles. They have provided some level of security and reassurance that when things go missing, we can easily find them. Now, these Bluetooth devices have been used to track our dogs, children, and even our ex-spouse without their knowledge or consent.

There is a significant risk of misuse of these devices. This includes stealth stalking of someone without them being aware of it. The lack of knowledge regarding technology can be easily exploited without proper knowledge of detecting these tracking devices. It is easy to see how coercive control, stalking, and harassment can be exacerbated by these devices being used for malicious purposes.

Our role is to ensure clients are informed as to how to detect these devices and how to protect themselves from future stalking.

A non-exhaustive checklist to provide your clients is as follows:

- Turn location services off on smart devices;
    - **On iOS**: Go to **Settings** > **Privacy & Security** > **Location Services**. Here, you can turn off location services entirely or adjust settings for individual apps to "Never" or "While Using the App."
    - **On Android**: Go to **Settings** > **Location**. You can toggle location services off or manage app permissions under **App permissions** to restrict access.
- Check settings within smart devices to restrict or revoke access to location services and restrict app permissions:
    - **On iOS**: In **Settings** > **Privacy & Security** > **Location Services**, you can see a list of apps and their location permissions.
    - **On Android**: Go to **Settings** > **Apps** > select an app > **Permissions** to manage location access.
- Check settings within smart devices to restrict or revoke access for specific apps with location services built into them:
    - **Google Maps**: Go to **Settings** > **Location Sharing** and turn it off.
    - **Social Media**: Check privacy settings for location sharing in apps like Meta/Facebook, Instagram, and Snapchat.
- Run an app to detect a Bluetooth device;
- Use a Virtual Private Network ("VPN") while browsing the internet;

- Disable Find My Device settings;
- Change passwords on any travel websites and third-party ride-share apps;
- Make sure the car your client drives is not connected to an app in control of the other party;
- Disconnect any shared fitness apps; and
- Ensure all accounts are set to private.

5.1 Types of Trackers

Overview of trackers (e.g., Apple AirTags, Samsung SmartTags, Tile)

Some of the most prevalent Bluetooth devices to track locations that connect to our mobile smart devices are the following:

- **Apple Airtag**: Bluetooth-based location device used to track items up to 100 meters, only compatible with iPhone, and includes anti-stalking features including notifications of unregistered AirTags being detected nearby.

- **Samsung SmartTags**: Bluetooth-based location device used to track items up to 120 meters, only compatible with Samsung smart devices, but lacks explicit anti-stalking features.

- **Tile**: Bluetooth-based location device used to track items up to 400 feet of range but lacks explicit anti-stalking features.

A quick search on Amazon provides numerous other alternative Bluetooth tracking devices that are more incognito. For example, credit card sized trackers. There are also multiple different concealing accessories for items such as Apple AirTags so that they can be easily attached to vehicles, insides of bags or jackets, or even the handlebar post of a bicycle. Therefore, our clients should have access to resources where they have learn how to detect these devices.

5.2 Safety Measures: Detecting and Disabling Trackers

Instructions for detecting and disabling trackers on various devices (e.g., Android 14's manual search, iOS 16's Safety Check feature)

i. Apple

Generally, any Apple device that has iOS 16 installed has a new "Safety Check" feature that allows the owner to manage who has access to their personal information, location, and devices. It is a quick way to revoke access for specific contacts and apps installed on the phone through the following settings:

- Emergency Reset – immediately revoke access for all shared information and resets privacy settings on the Apple device; and

- Manage Sharing and Access – provides a detailed breakdown of who has access to your information, location, calendar events, photos, and any other data. It allows you to selectively remove access on a contact-by-contact basis or app-by-app basis.

How to:

1. **Open Settings** and go to **Privacy & Security**.
2. Select **Safety Check**.
3. Choose between **Emergency Reset** or **Manage Sharing and Access**.
4. Follow on-screen prompts to review or change settings, ensuring your information is shared only with people and apps you trust.

ii. Android

Generally, newer Android devices have a "Manual Search" feature for detecting unknown Bluetooth tracking devices, including AirTags.

How to:

1. **Opening the Tracker Detection Tool**:
    a. Go to **Settings** on your Android device.
    b. Navigate to **Safety & Emergency**.
    c. Select **Unknown Tracker Alerts**.
2. **Initiating a Manual Scan:**
    a. Tap the Scan Now button to initiate a scan for nearby Bluetooth tracking devices.
    b. Android will start scanning for nearby trackers within range and list any detected devices that it identifies as potentially unknown or suspicious.
3. **Identifying Unknown Trackers:**
    a. If any unknown devices are found, Android will alert the user and provide details about the detected device (e.g., make and model of the tracker if identifiable).
    b. The user can then take further action, like locating the device if it's in close proximity, notifying authorities, or disabling the tracker (if possible

Use of applications such as Tracker Detect and AirGuard for detecting Bluetooth trackers

Generally speaking, AirTags and other Find My Devices (such as airpods) are perfect for tracking (most) Android users who will not be alerted by the AirTag being in close proximity and following them (unless they have access to the Manual Search feature outlined above). Therefore, the following apps have been frequently used to help Android users detect AirTags:

- The "Tracker Detect[33]" app allows Android users to scan for unknown AirTags in proximity.
- The "AirGuard"[34] app allows Android users to scan for unknown AirTags in proximity.

5.3 Monitoring Tool abuse

While parental monitoring apps can be valuable tools for ensuring child safety, their potential for misuse in contentious parenting situations is a significant concern. As alluded to previously, parental monitoring apps may be used for ulterior motives such as controlling, harassing, manipulating, or tracking the other party and their online activity, whether directly through the parent's device or the Child's device (which may be linked to the parent device) leading to misuse of monitoring access.

This can result in one parent having unauthorized access to the other's information without their consent, including messages, and only activity logs. Further, it can provide for constant remote surveillance of the other's location and activities, gaslighting, and manipulation to intimidate the other party.

5.4 Legal Implications of Unauthorized Tracking

Criminal liability for unauthorized use of tracking devices.

In Canada, section 264 of the *Criminal Code*[35] protects against Criminal Harassment. This section makes it a criminal offence to engage in harassing behaviour, including stalking or monitoring

---

33 Google Play Store, online <https://play.google.com/store/apps/details?id=com.apple.trackerdetect&hl=en>.

34 Google Play Store, online <https://play.google.com/store/apps/details?id=de.seemoo.at_tracking_detection.release&hl=en-AU>.

35 RSC 1985, c C-46.

someone's activities[36]. Recently, cyberstalking has fallen under criminal harassment as it becomes more prevalent with increasing online interactions.[37]

Sections 342.1, 342.2, and 430(1.1) of the *Criminal Code* prohibit the unauthorized use of a computer, interception of a computer system, the possession of a device to obtain unauthorized use of a computer system without permission, and mischief in relation to computer data. This includes hacking, intercepting, or stealing data, including using hacking software or devices. These sections make acts such as electronic eavesdropping and spy software illegal in nature.

6. Law Firm Cyber Protection

How to protect your firm from cyber security threats

Unfortunately, the legal profession has not yet moved towards a widely used uniform client management portal where information and communication can be securely exchanged with clients. Different industries, such as the medical industry, have multiple secure portal options available to professionals. Although there are some options available for the purposes of document exchange such as iManage's Closing Folders,[38] there is not one unified platform for KYC verification, written communication, video teleconferencing, and document storage and exchange that has been widely used by family law firms.

Clio Manage[39] has attempted to provide client management software that allows for encrypted file storage, permissions controls, and sharing with clients; however, it is inadequate with secure communications. This leaves counsel communicating with clients over email correspondence and multiple video teleconferencing technologies (Zoom, Teams, or Google Meet). Email correspondence lack encryption, allowing them to be easily intercepted with sensitive information, often ending up in the hands of a third-party. Therefore, it is incumbent on those operating legal practices to ensure that they are continuously improving their cyber security protocols in the absence of a confidential client portal.

---

36 Government of Canada, "Stalking is a crime called criminal harassment" (Dec 8, 2021), online <https://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/stalk-harc/har.html>.

37 Canlii, (2020), online <https://www.canlii.org/en/commentary/doc/2020CanLIIDocs3158?searchId=2024-10-25T16:17:57:002/c96eb56d2a4747cbad14bf274c080187&resultId=4f72b095adb747528c52785974f5d212&zoupio-debug#!fragment/zoupio-_Toc57359251/(hash:(chunk:(anchorText:zoupio-_Toc57359251),notesQuery:'',scrollChunk:!n,searchQuery:'%22criminal%20harassment%22%20AND%20%22cyber-stalking%22',searchSortBy:RELEVANCE,tab:search))>.

38 iManage: https://imanage.com/imanage-products/legal-transaction-management/closing-folders/

39 Clio Manage: https://www.clio.com/au/manage/

Cybercrimes are prevalent regardless of illegality. Firms can take steps to prevent cyber-attacks by[40]:

- engage a professional IT company to assist with cyber security;
- enroll in ALIA's Universal Cyber Coverage Program to provide resources to respond to cyberattacks and security breaches and obtain cybersecurity insurance[41][42];
- provide professional training to increase professional technological competence[43];
- educating employees on the appearance of scams and phishing activities;
- educating employees on email security – including not to open unexpected or untrusted email attachments[44];
- don't allow employees to use company email accounts for personal use;
- install spam filters;
- installing malware or AI powered cyber security software (such as SentinelOne);
- develop an incident response plan so everyone is aware of who to contact to resolve a cyber attack in the event that one occurs;
- implement a backup system with encryption of devices, networks and data storage;
- remote workers should use VPNs;
- remote workers should not work on open-source internet sources and instead use "hotspot" features on their mobile device;
- create cyber policies to be followed by all ream members to limit risk;
- regularly audit employee access to sensitive information;
- stringent email authentication protocols to verify legitimacy of messages/emails;
- establish strong passwords with complex passphrases and multi-factor authentication, while avoiding common password mistakes[45];

---

40 Law Society of Alberta, "Protecting Your Practice from Cybersecurity Threats" (Nov 3, 2023), online <https://www.lawsociety.ab.ca/protecting-your-practice-from-cybersecurity-threats/>.

41 Alberta Lawyers Indemnity Association, "Universal Syber Coverage Program", online <https://alia.ca/for-lawyers/cyber-coverage-program/>.

42 Alberta Lawyers Indemnity Association, "Universal Syber Coverage Program Update", online https://alia.ca/universal-cyber-coverage-program-update/.

43 Legal Education Society of Alberta, "Cybersecurity for Lawyers – Webinar" (Jun 15, 2020), online <https://www.lesaonline.org/program/cybersecurity-for-lawyers-webinar/>.

44 Inspired eLearning, "8 Email Security Best Practices You and Your Workforce Should Know", (2021), online <https://inspiredelearning.com/blog/email-security-best-practices/>.

45 Canadian Centre for Cyber Security – Government of Canada, "Best practices for passphrases and passwords" (Feb 2024), online <https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032>.

- and ensuring proper backup of private information. Outside risk assessments can be beneficial in targeting areas of improvement. Cyber security insurance can protect the firm if other prevention strategies fail.

As mentioned above, firms can conduct regular audits of their existing cybersecurity status, including an evaluation of:

- who and what is connected to their systems and networks;
- who has access to documents shared from their system;
- who is monitoring for risks;
- what is running on their systems and networks; and
- whether they have technology in place to prevent most breaches, rapidly detect breaches that do occur, and minimize the damage of such breaches.

7. Bibliography

PRIMARY MATERIALS – CASE LAW

***Criminal Code,* RSC 1985, c C-46.**

SECONDARY MATERIALS – ELECTRONIC SOURCES

Alberta Lawyers Indemnity Association, "Universal Syber Coverage Program", online <https://alia.ca/for-lawyers/cyber-coverage-program/>.

Alberta Lawyers Indemnity Association, "Universal Syber Coverage Program Update", online https://alia.ca/universal-cyber-coverage-program-update/.

Boston Children's Digital Wellness Lab, "Safety and Surveillance Software Practices as a Parent in the Digital World", (Nov 2023), online <https://digitalwellnesslab.org/research-briefs/safety-and-surveillance-software-practices-as-a-parent-in-the-digital-world/>.

Business Insider, Dave Johnson and Alexander Johnson, "What are deepfakes? How fake AI-powered audio and video warps our perception of reality" (Jul 25, 2023), online <https://www.businessinsider.com/guides/tech/what-is-deepfake>.

Canlii, (2020), online <https://www.canlii.org/en/commentary/doc/2020CanLIIDocs3158?searchId=2024-10-25T16:17:57:002/c96eb56d2a4747cbad14bf274c080187&resultId=4f72b095adb747528c52785974f5d212&zoupio-debug#!fragment/zoupio-_Toc57359251/(hash:(chunk:(anchorText:zoupio-_Toc57359251),notesQuery:'',scrollChunk:!n,searchQuery:'%22criminal%20harassment%22%20AND%20%22cyber-stalking%22',searchSortBy:RELEVANCE,tab:search))>.

Canadian Security Intelligence Service – Government of Canada, "Deepfakes: A Real Threat to a Canadian Future" (Nov 16, 2023), online <https://www.canada.ca/en/security-intelligence-service/corporate/publications/the-evolution-of-disinformation-a-deepfake-future/deepfakes-a-real-threat-to-a-canadian-future.html>.

Canadian Centre for Cyber Security – Government of Canada, "Best practices for passphrases and passwords" (Feb 2024), online <https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032>.

CBC, Amy Bell, "Oversharenting: Are you giving away too much about your kids online?" (Apr 24, 2019), online <https://www.cbc.ca/news/canada/british-columbia/parenting-online-social-media-oversharenting-1.5107340>.

Clinic to End Tech Abuse, "Resources", online <https://ceta.tech.cornell.edu/resources>.

Commissioner for Children & Young People, “Sharenting” (2018), online <https://www.ccyp.com.au/wp-content/uploads/2019/02/CCYP_2018.3.13_sharenting_infographic_final.pdf>.

Competition Bureau Canada – Government of Canada, “the rise of AI: Fraud in the digital age” (Mar 4, 2024), online <https://www.canada.ca/en/competition-bureau/news/2024/03/the-rise-of-ai-fraud-in-the-digital-age.html>.

Detsche Telekom, “Sharenting” (Jul 13, 2023), online (video): <https://youtu.be/FrdhsX8R_AY?si=w1V5aXl0vDzfT3py>.

eSafety Commissioner - Australian Government, “Cyberstalking”, online <https://www.esafety.gov.au/key-topics/staying-safe/cyberstalking>.

Global News, Callum Smith, “Monitoring child’s online activity is parental responsibility: RCMP” (Jan 3, 2019), online <https://globalnews.ca/news/4812608/monitoring-childs-online-activity/>.

Government of Canada, “Stalking is a crime called criminal harassment” (Dec 8, 2021), online <https://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/stalk-harc/har.html>.

IBM, “What is a digital footprint?”, online <https://www.ibm.com/topics/digital-footprint>.

Inspired eLearning, “8 Email Security Best Practices You and Your Workforce Should Know”, (2021), online <https://inspiredelearning.com/blog/email-security-best-practices/>.

Law Society of Alberta, “Protecting Your Practice from Cybersecurity Threats” (Nov 3, 2023), online <https://www.lawsociety.ab.ca/protecting-your-practice-from-cybersecurity-threats/>.

Legal Education Society of Alberta, “Cybersecurity for Lawyers – Webinar” (Jun 15, 2020), online <https://www.lesaonline.org/program/cybersecurity-for-lawyers-webinar/>.

Media Awareness Network, “Canada’s Children in a Wired World: The Parent’s View”, online <https://mediasmarts.ca/sites/default/files/pdfs/publication-report/full/YCWWI-parents-view.pdf>.

National Library of Medicine, “Sharenting; characteristics and awareness of parents publishing sensitive content of their children on online platforms”, (Jul 30, 2024), online <https://pmc.ncbi.nlm.nih.gov/articles/PMC11290302/#:~:text=Among%20parents%20using%20one%20or,their%20children%20on%20social%20media>.

Norton, “Cyberstalking: What it is and how to protect yourself” (Feb 28, 2024), online <https://us.norton.com/blog/how-to/what-is-cyberstalking>.

Oxford University Press, “Sharenting” (2022), online <https://www.oed.com/dictionary/sharenting_n>.

Statista, “Rate of identity thefts in Canada from 2012 to 2023” (July 2024), online, <https://www.statista.com/statistics/544904/identity-theft-rate-canada/>.

Statistics Canada – Government of Canada, “Women and men who experienced cyberstalking in Canada” (Jun 5, 2018), online <https://www150.statcan.gc.ca/n1/pub/75-006-x/2018001/article/54973-eng.htm>.

Telekom, “ShareWithCare: Telekom raises awareness for responsible use of children’s photos on the Internet” (Jul 3, 2023), online <https://www.telekom.com/en/company/details/share-with-care-telekom-raises-awareness-1041810>.

Telekom, “TeachToday”, online <https://www.teachtoday.de/en/>.

Vecanoi, “Very realistic Tom Cruise Deepfake / AI Tom Cruise (Feb 28, 2021), online (video) <https://youtu.be/iyiOVUbsPcM?si=TvIYFqM6WPNHJHLy>.

Victorian Klaw Reform Commission, “Stalking: Final Report – Responses to cyberstalking” (Oct 28, 2022), online <https://www.lawreform.vic.gov.au/publication/stalking-final-report/3-responses-to-cyberstalking/>.