

2-1-2016

Monitoring Your Teenagers' Online Activity: Why Consent or Disclosure Should be Required

Christina Nguyen

Seattle University School of Law, anguyen.christina@gmail.com

Follow this and additional works at: <https://digitalcommons.law.seattleu.edu/sjsj>



Part of the [Law Commons](#)

Recommended Citation

Nguyen, Christina (2016) "Monitoring Your Teenagers' Online Activity: Why Consent or Disclosure Should be Required," *Seattle Journal for Social Justice*: Vol. 15: Iss. 1, Article 15.

Available at: <https://digitalcommons.law.seattleu.edu/sjsj/vol15/iss1/15>

This Article is brought to you for free and open access by the Student Publications and Programs at Seattle University School of Law Digital Commons. It has been accepted for inclusion in Seattle Journal for Social Justice by an authorized editor of Seattle University School of Law Digital Commons.

Monitoring Your Teenagers' Online Activity: Why Consent or Disclosure Should be Required

Christina Nguyen

*Parents and legal guardians are permitted to monitor the computer, smartphone, and other electronic devices of children they are responsible for.*¹

—Amy Williams of TeenSafe

Author's Note: For the purposes of this article, the terms “teen” and “teens” as used below refer to individuals aged 13 through 17. The purpose of focusing on this particular age range was based on the specified age range under the Children’s Online Privacy Protection Act of 1998 (COPPA), which provides protections only for those below the age of 13.² Since the Federal Trade Commission did not provide the same protections for those aged 13 and above, it suggests that those aged 13 and above hold some level of autonomy regarding their online activities. While this will be discussed later in the article, it was necessary to first define the scope of “teen” and “teens” prior to its use. Any differentiations in identifying either “teen” or “teens” will be noted in the footnotes.

I. INTRODUCTION

Individual privacy is an important issue for most American citizens.³ Privacy can mean different things to different people. For some, privacy may mean protecting personal information, while for others, privacy may

¹ Amy Williams, *Is It Legal to Monitor Your Child With a Cell Phone Spy?*, TEENS SAFE (May 15, 2015), <http://www.teensafe.com/blog/legal-monitor-child-cell-phone-spy/>.

² *Children’s Online Privacy Protection Act (“COPPA”)*, FED. TRADE COMM’N, <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule> (last visited Apr. 1, 2016).

³ Mary Madden & Lee Rainie, *Americans’ Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. 4 (May 20, 2015), http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf.

mean keeping their communications private.⁴ The US Constitution grants some right of privacy to adults within their own home.⁵ However, minors⁶ do not similarly benefit from a right of privacy nor are they offered or guaranteed any right to privacy protection within the home.⁷ This is due, in part, to society's expectation for parents to use adequate means to protect their children, which may include monitoring the children's activities.⁸

Some parents have a "natural instinct . . . to want to protect their children from pain."⁹ Parents with that natural instinct generally want to know what their children are doing, i.e. where their children are, who their children are talking to, and what activities their children are participating in.¹⁰ When their children are not physically in the home, parents struggle to keep track of their children's activities.¹¹ However, even within the home, parents may

⁴ See Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CTR. 2-4 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

⁵ U.S. CONST. amend. IV.

⁶ "Minor" is defined as "a person who is not yet old enough to have the rights of an adult." "minor," MERRIAM-WEBSTER, <http://www.merriam-webster.com/dictionary/minor> (last visited Mar. 6, 2016). In Washington State, minors are any individuals less than 18 years old. WASH. REV. CODE § 26.28.010 (1971).

⁷ Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759, 759-60 (2011).

⁸ *Id.* at 761.

⁹ See Katie Russell, *I Can't Always Protect My Child – and I Don't Always Want To*, HUFFPOST PARENTS (June 4, 2014, 1:50 PM), http://www.huffingtonpost.com/kate-russell/i-cant-always-protect-my-children-and-i-dont-always-want-to_b_5025846.html.

¹⁰ See Lori Grisham, *Teen Tracking Apps: Good Parenting or Risky?*, USA TODAY (Sept. 18, 2014, 12:32 AM), <http://www.usatoday.com/story/tech/personal/2014/09/17/teens-parents-tracking-apps-security-mamabear-teensafe/15716335/> ("If we don't know what is going on in their digital world we can't protect them, we can't guide them").

¹¹ See, e.g., Stephen N. Roberts, *Tracking Your Children With GPS: Do You Have The Right?*, FINDLAW, <http://corporate.findlaw.com/law-library/tracking-your-children-with-gps-do-you-have-the-right.html> (last visited Apr. 3, 2016) ("Parents may not be able to keep their children in sight at all times").

struggle due to advancements in technology and use of electronic devices.¹² Recent generations are growing up in the digital age, so they are likely to be more technologically savvy than older generations.¹³ Because of their familiarity with technology, most teens tend to not worry about other people seeing what they are doing online.¹⁴ Unbeknownst to many of those teens, some parents use monitoring applications or programs to not only track their teens' locations but also their teens' web activity, text messages, social media profiles, etc.¹⁵

On one hand, minors are a group that both society and the government have a special interest in protecting.¹⁶ Teen brains, while more developed than younger children's brains, are still "works in progress."¹⁷ Scientific research has established that teens are still lacking in certain areas including decision-making, impulse control, and long-term planning.¹⁸ Due to this incomplete development, teens are more susceptible to making poor

¹² See Jeffrey S. Dill, *Why Parents Worry About Technology, But Struggle to Limit Its Use*, FAMILY STUDIES (Mar. 3, 2014), <http://family-studies.org/why-parents-worry-about-technology-but-struggle-to-limit-its-use/>.

¹³ See Patricia Reaney, *Young Teens More Tech Savvy, Pragmatic Than Older Millennials (STUDY)*, HUFFINGTON POST (June 16, 2013, 4:04 PM), http://www.huffingtonpost.com/2013/06/19/teens-tech-mtv-study_n_3467960.html (citing a study done by MTV Insights, a research group of one of Viacom Inc.'s American cable television channel).

¹⁴ See *id.* ("About 70 percent of teens said they have the freedom to go anywhere they want online").

¹⁵ Gina Gaston, *Parents Use Apps to Track Child's Cell Phone, Social Media Accounts*, ABC13 EYEWITNESS NEWS (Dec. 15, 2014), <http://abc13.com/family/parents-use-apps-to-track-childs-cell-phone-online-accounts/437391/>.

¹⁶ See Eugene Volokh, *Freedom of Speech, Shielding Children, and Transcending Balancing*, 1997 SUP. CT. REV. 141 (1997) ("The government has a strong interest in shielding children from unsuitable—because sexually explicit or (perhaps) profane—speech"); see also *Major Federal Legislation Concerned with Child Protection, Child Welfare, and Adoption*, CHILDREN'S BUREAU (Apr. 2012), <https://www.childwelfare.gov/pubpdfs/majorfedlegis.pdf> (demonstrating an intention to protect children on a national level).

¹⁷ *Teen Brains Are Not Fully Developed*, CAMPAIGN FOR YOUTH JUST. 1, http://www.campaignforyouthjustice.org/documents/Teen_Brains_Are_Not_Fully_Developed.pdf (last visited Nov. 23, 2015).

¹⁸ *Id.*

decisions,¹⁹ and society acknowledges that someone must be responsible for guiding teen lives and steering teens toward the right track.²⁰ Courts and lawmakers recognize that parents are not only able to protect their children, but are the best option for doing so.²¹ Thus, society and the government generally allow parents to choose their own child-rearing methods with little interference.²²

On the other hand, teens deserve a right to privacy when using their electronic devices. When parents and society aim to protect children, they might monitor teens' personal communications, social media activity, and other related information without the teen's consent. This type of monitoring may be harmful to teens because it can hinder trust development, obstruct communication with parents, force LGBTQ+ teens²³ into "coming out,"²⁴ and negatively affect overall mental health. Yet parents in Washington State are not legally required to inform their teens if they are

¹⁹ See Susan S. Lang, *Why Teens Do Stupid Things: They Think More than Adults Do About Risks and Benefits, But then Opt for the Benefits*, CORNELL CHRONICLE (Dec. 4, 2006), <http://www.news.cornell.edu/stories/2006/12/why-teens-do-stupid-things> (quoting Valerie F. Reyna, professor of human development at Cornell, who says that teens decide that the benefits of their behavior outweigh the risks); see also Danica Davidson, *Why Do Teenagers Make Bad Choices? One Word: Science*, MTV NEWS (Mar. 4, 2015), <http://www.mtv.com/news/2094754/one-bad-choice-teenage-brains/> (discussing the theory that the brain is not fully developed until the teen is past the age of 20).

²⁰ See, e.g., Justin W. Patchin, *Holding Parents Responsible for Their Child's Bullying*, CYBERBULLYING RES. CTR. (June 17, 2013), <http://cyberbullying.org/holding-parents-responsible-for-their-childs-bullying/>.

²¹ See Shmueli & Blecher-Prigat, *supra* note 7, at 761-62 (citing *Parham v. J.R.*, 442 U.S. 584, 602 (1979)) ("courts believe that a 'parent possess[es]' what a child lacks in maturity, experience and capacity for judgment required for making life's difficult decisions.").

²² See *id.* at 762.

²³ "LGBTQ" refers to Lesbian, Gay, Bisexual, Transgender, and Questioning or Queer. The "+" refers to all unnamed sexual orientations and gender identities including, but not limited to, asexual, pansexual, gender-nonconforming.

²⁴ See *The Coming Out Process*, CAL. ST. UNIV. LONG BEACH, <http://web.csulb.edu/colleges/chhs/safe-zone/coming-out/> (last visited Nov. 23, 2015) ("The term 'coming out' of the closet refers to the life-long process of the development of a positive gay, lesbian, bisexual, or transgender identity.").

using this type of monitoring.²⁵ However, parents who tell their teens they are using monitoring applications or programs, and/or obtain their teens' consent to use such things, could benefit from the supplementary parenting device.

The Washington State Legislature should undertake the following three suggestions to balance the need for teen privacy rights with the need to protect teens from outside harm: (1) extend the scope of Washington's two-party consent²⁶ requirement for the Washington Privacy Act's electronic communications section²⁷ to include parents' use of monitoring tools, (2) apply the "announcement" standard²⁸ for consent in the electronic communications section to obtaining consent to use monitoring tools from parties that are not the parents' own teen, and (3) require monitoring tool distributors²⁹ to ensure two-party consent is achieved before parental use by establishing new legislation outlining the specific requirements for monitoring tool distributors to abide by, including minimum recordkeeping standards.

This article will discuss the following issues relating to the need for the Washington State Legislature to adopt the three aforementioned suggestions. Section II of this article will discuss the rise in teen use of electronic devices, including an increased access to the internet and use of social media websites. Section III will discuss the use of monitoring applications and programs, including the difference between tracking and

²⁵ Washington currently has no specific laws addressing whether parents are legally allowed to use monitoring applications on their children's mobile devices.

²⁶ Technically, Washington's requirement is "all-party consent." For the purposes of applying it to the use of monitoring tools, the term "two-party consent" is used to refer to consent from the parent and the teen. Note that this form of dual consent would be different from the all-party consent because it does not require consent from the other individual party to the communication or conversation.

²⁷ WASH. REV. CODE § 9.73.030(1) (1986) (also known as Washington's "wiretapping law").

²⁸ WASH. REV. CODE § 9.73.030(3) (1986).

²⁹ The title "monitoring tool distributor" or "distributor of monitoring tools" as used in this article is meant to include those who provide access to the monitoring tools.

monitoring and the different types of applications and programs for each. Section IV will discuss how a lack of teen privacy affects other aspects of family life. The section will explore the potential negative effects of parents monitoring their teen(s). Section V will discuss the current legislation protecting privacy rights in other areas that could be applied to teens. Section VI will further expand on the three aforementioned suggestions and explain why the Washington State Legislature should implement them. Finally, Section VII will discuss potential arguments opposing a two-party consent requirement for parental use of monitoring tools.

II. THE RISE IN TEEN USE OF MOBILE DEVICES, COMPUTERS, AND TABLETS

A majority of teens today have or have access to a mobile phone.³⁰ From 2004 to 2010, the percentage of teens with mobile phones rose from approximately 45 percent to approximately 75 percent, a total increase of about 30 percent.³¹ Since 2010, that number has continued to increase—in 2015, approximately 88 percent of teens owned or had access to some type of mobile phone.³² Similar statistics exist for teen access to computers or tablets—in 2015, approximately 87 percent of teens owned or had access to a desktop or laptop computer while approximately 58 percent of teens owned or had access to a tablet computer.³³

³⁰ Amanda Lenhart, *Teens, Social Media & Technology Overview 2015*, PEW RES. CTR. 2, 8 (Apr. 9, 2015), http://www.pewinternet.org/files/2015/04/PI_TeensandTech_Update2015_0409151.pdf (indicating that, in a survey of 1,060 teens aged 13 to 17, almost three-quarters of teens “have or have access to” a smartphone, about 30 percent have a basic phone, and about 12 percent have no phone at all).

³¹ Amanda Lenhart, et al., *Teens and Mobile Phones*, PEW RESEARCH CENTER 2 (Apr. 20, 2010), <http://www.pewinternet.org/files/old-media/Files/Reports/2010/PIP-Teens-and-Mobile-2010-with-topline.pdf> (this particular statistic references those individuals aged 12 to 17 as opposed to individuals aged 13 to 17) [hereinafter *Teens and Mobile Phones*].

³² Lenhart, *supra* note 30, at 8.

³³ *Id.* at 10.

Teens commonly access mobile devices for a variety of reasons, including keeping them safe in case of emergencies, communicating with family and friends, learning and practicing responsibility, and doing homework.³⁴ One of the major appeals of mobile devices to teens is the variety of methods with which teens can communicate.³⁵ For many teens, texting is an important form of communication³⁶—approximately 90 percent of teens with access to a mobile device send text messages.³⁷ While teens may use the texting application their mobile device provides, many teens also download other messaging applications to their phone, such as Kik, WhatsApp, Facebook Messenger, and Line.³⁸

A. Teens' Access to the Internet and Use of Social Media Have Increased

More teens these days use mobile devices and computers, which has led to increased access to the internet and social media compared to teens that do not use those devices.³⁹ On average, teens with mobile devices access the internet more often than those who do not own mobile devices.⁴⁰ An overwhelming 92 percent of teens reported going online daily, while 24 percent of those teens indicated they went online “almost constantly.”⁴¹

³⁴ See Robert Myers, *The Pros and Cons of Giving a Mobile Phone to Your Teenager*, CHILD DEV. INST. (Jan. 4, 2015), <http://childdevelopmentinfo.com/parenting/pros-cons-giving-mobile-phone-teenager/>.

³⁵ See Lenhart, *supra* note 30, at 4 (“As American teens adopt smartphones, they have a variety of methods for communication and sharing at their disposal.”).

³⁶ See *id.* at 4 (“Texting is an especially important mode of communication for many teens.”).

³⁷ *Id.*

³⁸ *Id.* at 4-5; see generally Parmy Olson, *Facebook's Dominance in Messaging Has Crushed LINE's Valuation*, FORBES (June 3, 2016, 11:14 AM), <http://www.forbes.com/sites/parmyolson/2016/06/03/facebook-messaging-line-ipo/#3bd1ec92409b>.

³⁹ See Lenhart, *supra* note 30, at 2 (finding that most teens with mobile phones use the internet more often than those without mobile phones).

⁴⁰ *Id.*

⁴¹ *Id.*

Additionally, most teens use more than one social media website.⁴² Facebook, Instagram, and Snapchat made up the top three social media platforms that teens aged 13 to 17 used between October 2014 and March 2015.⁴³ Other prominent social media platforms teens used included Twitter, Google+, Vine, and Tumblr.⁴⁴ Social media has become such a pervasive part of teen life that many teens are unable to imagine their lives without it.⁴⁵ As such, teens are now spending more time online and on social media than ever before.⁴⁶

Teens use social media for a variety of reasons—some use it as a news source,⁴⁷ while others use it to communicate with people online.⁴⁸ Instead of reading the newspaper, watching the news on television, or searching news websites for articles, teens often use social media websites such as Facebook and Twitter as their preferred news source.⁴⁹ Social media websites provide platforms for teens to facilitate discussion and share their opinions on current events.⁵⁰ Going online or using social media have become activities for teens to cure boredom.⁵¹ Some teens even use social media to promote their own brands or businesses.⁵² Despite the many

⁴² *Id.* at 3.

⁴³ *Id.* (Approximately 71 percent reported using Facebook, approximately 52 percent reported using Instagram, and approximately 41 percent reported using Snapchat).

⁴⁴ *Id.* at 2.

⁴⁵ See Alan Jones, *Teens 'Can't Live without Smartphones and Social Media,'* THE SCOTSMAN (Oct. 27, 2015, 2:49 PM), <http://www.scotsman.com/news/teens-can-t-live-without-smartphones-and-social-media-1-3929363>.

⁴⁶ See Mariah Miller, *Teens Filling Time with Social Media*, KPCNEWS (Nov. 22, 2015, 1:15 AM), http://www.kpcnews.com/features/special/kpcnews/article_d57c30e1-3ef8-5261-8284-9c46b10b5fbd.html.

⁴⁷ See *id.*

⁴⁸ *Id.*

⁴⁹ See *id.*

⁵⁰ *Id.*

⁵¹ See *id.*

⁵² See Jaylen Bledsoe, *Using Social Media As a Teenager*, HUFFPOST TEEN (July 23, 2014, 12:13 PM), http://www.huffingtonpost.com/jaylen-bledsoe/using-social-media-as-a-t_b_5375487.html (Bledsoe is a 17-year-old teen that uses Twitter, Facebook, and Instagram to reach out to celebrities and non-profit organizations).

positive reasons teens use the Internet and social media, parents have voiced concerns about their teens' exposure to the dangers of the digital world.⁵³

B. Parental Concern for Teen Safety with Increased Access to the Internet and Social Media

While teen use of the Internet and social media has become standard, parents remain concerned about “the behaviors teens engage in online, the people with whom they interact and the personal information they make available.”⁵⁴ Among some of the greatest concerns parents have are online sexual predators and teen bullying.⁵⁵ One study found that teens aged 13 to 17 were particularly vulnerable to Internet-initiated sex crimes.⁵⁶ Some parents credit these concerns to their children's trusting natures—one parent stated that “children are so trustworthy [of] these modern technologies that they sometimes neglect the fact that it can cause harm to them.”⁵⁷ However, parents may not always take further measures to teach their children Internet safety.⁵⁸

⁵³ See Monica Anderson, *Parents, Teens and Digital Monitoring*, PEW RES. CTR. 2 (Jan. 7, 2016), http://www.pewinternet.org/files/2016/01/PI_2016-01-07_Parents-Teens-Digital-Monitoring_FINAL.pdf.

⁵⁴ *Id.*

⁵⁵ See City of Milwaukie, *Internet and Cellular Phone Usage - Safety Concerns for Parents*, <http://www.milwaukieoregon.gov/police/internet-and-cellular-phone-usage-safety-concerns-parents> (last visited Mar. 6, 2016) (stating the most common incidents relating to “children's Internet and cellular phone activities” reported to police in Milwaukie, Oregon were children being victimized sexual predators and teens being harassed through texting and verbal threats).

⁵⁶ See Janis Wolak et al., *Online “Predators” and Their Victims: Myths, Realities, and Implications for Prevention and Treatment*, 2008 AMERICAN PSYCHOLOGIST 115 (Mar. 2008), <http://www.apa.org/pubs/journals/releases/amp-632111.pdf>.

⁵⁷ See Mark Pace, *Parents See Online Dangers*, WASH. TIMES (Nov. 12, 2014), <http://www.washingtontimes.com/news/2014/nov/12/parents-and-internet-parents-see-online-dangers/>.

⁵⁸ See, e.g., Family Online Safety Institute (FOSI), *Parenting in the Digital Age: How Parents Weigh the Potential Benefits and Harms of Their Children's Technology Use 2* (Nov. 12, 2014), <https://www.fosi.org/policy-research/parenting-digital-age/>.

Although almost all parents discuss the dangers of the Internet with their teens, one out of three admit they do not discuss the topic with their teen regularly.⁵⁹ Advising teens about the potential dangers of the Internet is one of the more prevalent pieces of advice given to parents regarding their teens' online safety.⁶⁰ While parents talking to their teens about Internet danger will not guarantee teen safety, more frequent conversation may increase the chances of teens being more informed and better equipped to handle unwanted online advances.⁶¹ In addition to talking to teens about online safety, parents also use monitoring tools to track teens' mobile phone and computer activity.⁶²

III. MONITORING APPLICATIONS AND PROGRAMS

Most people are familiar with the Global Positioning System (GPS) type of tracking; GPS tracking has become commonplace, particularly with the use of mobile phones.⁶³ While people may also be familiar with mobile phone and computer monitoring applications and programs, teens may find it unlikely that their parents are using them on their devices.⁶⁴ These tools

⁵⁹ *Id.*

⁶⁰ See, e.g., *A Parent's Guide to Internet Safety*, FED. BUREAU OF INVESTIGATION: CYBER DIVISION, 4, <https://www.fbi.gov/stats-services/publications/parent-guide/parentsguide.pdf> (last visited Mar. 6, 2016); *Kids' Online Safety*, FED. TRADE COMMISSION (FTC), <https://www.consumer.ftc.gov/topics/kids-online-safety> (last visited Mar. 6, 2016).

⁶¹ See *Talking to Kids and Teens About Social Media and Sexting*, AM. ACAD. OF PEDIATRICS (May 31, 2013), <https://www.aap.org/en-us/about-the-aap/aap-press-room/news-features-and-safety-tips/pages/Talking-to-Kids-and-Teens-About-Social-Media-and-Sexting.aspx> (providing tips emphasizing the importance of getting teens to understand the various dangers online).

⁶² See Anderson, *supra* note 53 (39 percent of parents reported using parental controls to block, filter, or monitor their teen's online activity).

⁶³ See Stephen Lawson, *Ten Ways Your Smartphone Knows Where You Are*, PCWORLD, (Apr. 6, 2012), http://www.pcwORLD.com/article/253354/ten_ways_your_smartphone_knows_where_you_are.html.

⁶⁴ See Regan Morris, *Child Watch: The Apps That Let Parents 'Spy' on Their Kids*, BBC NEWS (Jan. 29, 2015), <http://www.bbc.com/news/technology-30930512> (a random group

come in many forms and can be much more detailed than simply looking at an individual device's browsing history. While a person viewing another person's browser history can see what websites that other person visited, a person using monitoring tools can view any messages sent and received (e-mails, texts, messages through other applications),⁶⁵ as well as social media posts.⁶⁶ Despite violating a person's privacy, use of monitoring tools is not uncommon.⁶⁷ There are even websites providing lists of monitoring applications and programs that are well regarded, with some applications and programs specific to teen monitoring.⁶⁸

One of the major selling points for these tools is that people may use them covertly, i.e. without the person they are monitoring knowing.⁶⁹ Many of the websites for monitoring tools advertise the discreteness or the concealed nature as a key feature of the product.⁷⁰ Producers of monitoring tools advertise different features.⁷¹ Some common features include

of teens in Los Angeles believed it was "highly unlikely" that their parents were spying on them).

⁶⁵ These applications include Kik, Whatsapp, and other messaging applications.

⁶⁶ WEBWATCHER, <http://www.webwatcher.com/> (last visited Nov. 23, 2015); TEENSAFE, <http://www.teensafe.com/> (last visited Nov. 23, 2015). Viewing of social media profiles require parents to have the teen's login information. See WEBWATCHER, *supra*; TEENSAFE, *supra*.

⁶⁷ See Gaston, *supra* note 15.

⁶⁸ See Brian S. Hall, *Best Parental-Control Apps 2015*, TOM'S GUIDE (Jun. 24, 2016), <http://www.tomsguide.com/us/best-parental-control-apps,review-2258.html>; see also Purch, *2016 Best Monitoring Software Review*, TOPTENREVIEWS, <http://monitoring-software-review.toptenreviews.com/> (last visited Nov. 23, 2015); see also Ann Brenoff, *5 Apps to Spy On Your Kids Without Them Knowing*, HUFFINGTON POST (July 29, 2015, 07:59 AM), http://www.huffingtonpost.com/entry/how-to-track-your-kids-without-them-knowing-youre-on-their-tail_55afaff1e4b07af29d56f544.

⁶⁹ See WEBWATCHER, *supra* note 66 (listing "Discrete/Tamper Proof" as one of the main features—"By design, WebWatcher is undetectable . . ."); see also *SpyAgent Invisibly Logs Everything Users Do*, SPYTECH, <http://www.spytech-web.com/index.shtml> (last visited Aug. 4, 2016) ("SpyAgent's unmatched feature-set invisibly monitors all computer usage and internet activity.").

⁷⁰ See WEBWATCHER, *supra* note 66; see also *SpyAgent Invisibly Logs Everything Users Do*, *supra* note 69.

⁷¹ See, e.g., WEBWATCHER, *supra* note 66; TEENSAFE, *supra* note 66; *Ultimate Monitoring Tool for All Devices*, *infra* note 72.

accessibility, monitoring multiple devices, and monitoring remotely.⁷² Many monitoring tools are created for use by parents to monitor their children or by employers to monitor their employees.⁷³ Use of monitoring tools is allowed in employer-employee settings mainly due to a lack of laws regulating employees' electronic activity in the workplace.⁷⁴ Similarly, use of monitoring tools is permitted in families with underage children because courts tend to stay out of family privacy matters.⁷⁵ Some parents believe monitoring their children correlates with "good parenting."⁷⁶ While some applications operate covertly, others are clearly visible on the teen's mobile device.⁷⁷ These programs are designed to work on mobile phones, computers, or both, and include TeenSafe, MamaBear, WebWatcher, and Spytech SpyAgent, all of which are discussed below.⁷⁸

⁷² See *Ultimate Monitoring Tool for All Devices*, MSPY, http://www.mspy.com/?AVGAFFILIATE=3305&_c=1&utm_expId=77466971-65.7YjuDz5oQrOxt9M8DnEDSA.0&utm_referrer=http%3A%2F%2Fwww.huffingtonpost.com%2Fentry%2Fhow-to-track-your-kids-without-them-knowing-youre-on-their-tail_55afaff1e4b07af29d56f544 (last visited Nov. 23, 2015).

⁷³ See Brenoff, *supra* note 68.

⁷⁴ *Privacy in America: Electronic Monitoring*, AM. C.L. UNION, <https://www.aclu.org/privacy-america-electronic-monitoring> (last visited Nov. 23, 2015). A couple of states do require employers to disclose to employees when they use monitoring tools and the types of monitoring being done (Connecticut and Delaware). Colorado and Tennessee require states and public entities to have policies informing employees that electronic mail communications are subject to inspection. *State Laws Related to Internet Privacy*, NAT'L CONF. OF ST. LEGISLATURES (Feb. 24, 2015), <http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#Monitoring>.

⁷⁵ Shmueli & Blecher-Prigat, *supra* note 7, at 761-62.

⁷⁶ See Grisham, *supra* note 10; see also Kelly Wallace, *Brutally Honest: Is It OK to Spy on Your Kids?*, CNN (Jan. 13, 2015, 11:07 AM), <http://www.cnn.com/2015/01/06/living/feat-brutally-honest-parenting-spying/> (a mom of three boys in Maryland stated "I don't call it spying. I call it parenting").

⁷⁷ TeenSafe and WebWatcher work covertly, while MamaBear is visible on the mobile device. TEENSAFE, *supra* note 66; WEBWATCHER, *supra* note 66; MAMABEAR, *infra* note 95.

⁷⁸ The applications discussed in this article were chosen primarily because they were mentioned in articles discussing whether parents should use spying applications on their children.

A. TeenSafe

TeenSafe is a monitoring service created specifically for parents to monitor teens' mobile phone activity.⁷⁹ It is designed to work on either an iPhone⁸⁰ or Android smartphone, with certain features exclusive to each device.⁸¹ For instance, viewing sent and received messages on Whatsapp or Kik is only available for iPhone devices, while viewing installed applications is only available for Android devices.⁸² TeenSafe is a subscription-based service, so parents pay a monthly fee to use the service.⁸³ The TeenSafe creators advocate for the service as a method of keeping teens safe—their tagline is “Protecting Your Most Valuable Treasure.”⁸⁴ In line with that overarching goal, TeenSafe creators assert the service is “Parenting Empowered,” adding that the service is “built by Parents *for* Parents.”⁸⁵

The five main features TeenSafe advertises are as follows: (1) viewing sent, received, and deleted SMS (short message service) and iMessages; (2) viewing call logs of incoming and outgoing calls, including the person's contact name, number, the date the call was placed, and the call's duration;⁸⁶ (3) seeing the phone's current and prior geographical location; (4) viewing Instagram posts, comments, and followers; and (5) viewing what third-party applications are on the phone.⁸⁷ Other features TeenSafe boasts are the abilities to view sent and received Whatsapp and Kik

⁷⁹ TEENS SAFE, *supra* note 66.

⁸⁰ Using TeenSafe with an iPhone requires the Apple ID and password, which is likely to be easy to obtain if the parent buys the iPhone for their teen. For iPads and the iPod touch, these are likely to be shared devices with a common Apple ID and password.

⁸¹ TEENS SAFE, *supra* note 66.

⁸² *Id.*

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ The only thing differentiating this feature from a person looking at phone records is the ability to see the contact name.

⁸⁷ TEENS SAFE, *supra* note 66. The fifth feature is exclusive to Android phones.

messages and messenger texts,⁸⁸ web search history, web browsing history, and contacts.⁸⁹ However, TeenSafe does not work with all mobile devices—it is available for iPhone and Android phones, as well as for iPads and the iPod touch, but it does not work with Blackberry or Windows phones.⁹⁰

TeenSafe creators believe that monitoring is mandatory because the digital era exposes teens to many dangers such as cyberbullying, sexting, online predators, and accessing sexually explicit content.⁹¹ However, they do not definitively state whether parents should disclose use to teens.⁹² Within the page's "Frequently Asked Questions" section, TeenSafe responds to whether teens need to know their parents are using TeenSafe with the following passage:

Parents and Guardians have a legal right to monitor their children under the age of 18 if they pay the phone bill. Every parent's situation is unique and only a parent can decide whether to inform their teen of their intent to use TeenSafe. Many parents choose to tell their teen that they're using TeenSafe. This choice is, however, entirely up to the discretion of the parent.⁹³

While not explicitly saying parents should tell their teens they are using the application, TeenSafe does stress communication as the foundation to keeping teens safe.⁹⁴

B. MamaBear

While offering the same services as other monitoring applications, MamaBear differs from other applications in fundamental ways.⁹⁵ Unlike

⁸⁸ This is exclusive to iPhones.

⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ Amy Williams, *The TeenSafe Parenting Guide to Tech Safety*, TEENS SAFE (Nov. 21, 2014), <http://www.teensafe.com/blog/teensafe-parenting-guide-tech-safety/>.

⁹² TEENS SAFE, *supra* note 66.

⁹³ *Id.*

⁹⁴ Williams, *supra* note 91.

⁹⁵ MAMABEAR, <http://mamabearapp.com/> (last visited Apr. 3, 2016).

TeenSafe, MamaBear cannot be used covertly—the application is not only visible on the teen’s mobile device but needs to remain there for the parent to receive information.⁹⁶ This possibly eliminates the lack of disclosure by making the application’s presence known. Unless teens remain oblivious to the application on their mobile device, teens are likely to notice it and be aware of their parents’ monitoring activity. MamaBear offers the following features: (1) tracking a teens location, alerting parents when teens arrive or leave certain places; (2) viewing social media activity;⁹⁷ (3) viewing all incoming and outgoing text messages; and (4) alerting parents when teens are speeding.⁹⁸

C. WebWatcher

WebWatcher is software designed to monitor computers and mobile phones.⁹⁹ This software works with PC, Mac, iPhone, Android, and Blackberry devices.¹⁰⁰ On its website, WebWatcher is advertised as the “#1 rated Parental & Employee Monitoring Software.”¹⁰¹ Like TeenSafe, WebWatcher is designed to be undetectable to the person being monitored.¹⁰² The software works by recording all activity on the computer and sending it to a secure web-based account where parents can monitor activity from any computer.¹⁰³ WebWatcher offers different features for each device, with PC and Mac devices offering the most features.¹⁰⁴

⁹⁶ *Frequently Asked Questions*, MAMABEAR, <http://mamabearapp.com/about/faqs/> (last visited Nov. 23, 2015).

⁹⁷ The social media platforms MamaBear allows monitoring for are Instagram, YouTube, Facebook, and Twitter. Login information for these platforms is required in order for parents to monitor activity.

⁹⁸ *Features*, MAMABEAR, <http://mamabearapp.com/app-features/> (last visited Nov. 23, 2015).

⁹⁹ WEBWATCHER, *supra* note 66.

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ *Id.*

In addition to the usual features monitoring applications and programs offer, WebWatcher sends notifications when certain “alert words” appear on a teen’s or employee’s device.¹⁰⁵ At the bottom of their website, Awareness Technologies—the corporation that created WebWatcher—has a disclaimer requiring software users to inform people their computer activity is being monitored.¹⁰⁶ However, this may apply only to employer-employee relationships since there are no federal or state laws requiring parents to disclose use.¹⁰⁷

D. Spytech SpyAgent

Spytech SpyAgent¹⁰⁸ is another example of monitoring software, boasting that one of its main features is stealth.¹⁰⁹ As evidenced by its name, Spytech SpyAgent was designed to be spy software with a multitude of different features.¹¹⁰ Spytech SpyAgent takes pride in the fact that the software is “undetectable under all Windows versions . . . and can circumvent popular third-party ‘spyware’ detectors.”¹¹¹

Spytech SpyAgent lists a number of activities it is able to log as compared to other monitoring applications or programs.¹¹² Some of these activities include keystroke monitoring, emails sent and received, internet chat conversations,¹¹³ website activity, application usage, and files created, accessed, modified, or deleted. In addition to being monitoring software,

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ The disclaimer states that failure to inform of monitoring activity may “result in breaking of Federal and State laws.” *Id.* Awareness Technologies is a company with its headquarters in Connecticut; Connecticut is one of two states that explicitly require employers to disclose when they are using computer-monitoring tools.

¹⁰⁸ *Spy Agent – stealth and undetectable monitoring software*, SPYAGENT, <http://www.spyagent.net/> (last visited Nov. 23, 2015).

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² *Id.*

¹¹³ These include AOL, AOL Instant Messenger, AIM Triton, Yahoo Messenger, MSN Messenger, Excite Messenger, GoogleTalk, Skype, XFire, and ICQ.

Spytech SpyAgent also acts as a filter to prevent the user from visiting certain websites or using certain applications.¹¹⁴

E. The Difference Between Tracking and Monitoring: Why It Matters

While both tracking and monitoring invade a person's privacy, tracking is fundamentally different from monitoring the person's mobile device or computer activity—tracking is like seeing where a person is physically on the street, while monitoring is like seeing what is going on inside that person's head. While both types of activities may be harmful, in fictional stories, characters with the ability to read minds are often considered more dangerous due to the invasive nature of their power.¹¹⁵ People rightfully believe that what goes on inside of their head is for them only—that is why people think to themselves. The same holds true when people direct their comments toward another individual—93 percent of adults believe it is important to be in control of who can get information about them, while 93 percent of adults also believe it is important to “hav[e] the ability to share confidential matters with another trusted person.”¹¹⁶ The bottom line is that people, including teens, want the ability to keep certain things to themselves.

Teens are especially justified in wanting this privacy considering the mental and physical changes they experience during puberty.¹¹⁷ Monitoring applications allow parents to gain access to their teens' thoughts, which they would not have access to otherwise. Therefore, while parents knowing their teens' location can be displeasing to most teens, having parents pry into their private activities and discussions without them knowing could

¹¹⁴ *Spy Agent*, *supra* note 108.

¹¹⁵ See, e.g., *Teen Titans: Nevermore* (Cartoon Network television broadcast, Aug. 30, 2003) (In *Teen Titans*, Raven responded negatively to the other members entering her mind).

¹¹⁶ Madden & Rainie, *supra* note 3, at 4.

¹¹⁷ See Denise Witmer, *Why Do Teens Need Privacy From Their Parents?*, VERY WELL, <https://www.verywell.com/why-does-my-teen-need-privacy-2609615> (last visited Apr. 3, 2016).

result in more negative effects, particularly if the teens find out unintentionally. Monitoring teens with these applications and programs is as invasive as mind reading, particularly because parents can read messages that were never meant for them.¹¹⁸

IV. POTENTIAL NEGATIVE IMPACT OF USING MONITORING APPLICATIONS AND PROGRAMS ON TEENS

Parents' use of monitoring applications and programs to keep an eye on their teens without those teens' disclosure could potentially create more detriments than benefits. First, hiding this type of monitoring from teens could result in major negative impacts to teens generally, such as stunting trust development and effective familial communication.¹¹⁹ Second, parents hiding the monitoring of their teens may also result in negative impacts to LGBTQ+ teens in particular, including narrowing the limited safe spaces that LGBTQ+ teens have and potentially causing a forced coming out.¹²⁰ Finally, parents hiding their teen monitoring may heighten the risk of teens

¹¹⁸ Assuming that individuals go in for mind reading services voluntarily, those individuals would necessarily open their thoughts to the mind reader; while still potentially violating, the individual would have consented to this behavior.

¹¹⁹ See Tonya Rooney, *Spying on your kid's phone with Teensafe will only undermine trust*, PHYS.ORG (Apr. 29, 2015), <http://phys.org/news/2015-04-spying-kid-teensafe-undermine.html>.

¹²⁰ See Elizabeth Hunter, *Is the Rise of Digital Media Helping, or Hurting, Queer Youth?*, FLIP THE MEDIA (Nov. 1, 2010), <http://flipthemedias.com/2010/11/is-the-rise-of-digital-media-helping-or-hurting-queer-youth/> ("The internet is so profound in queer youth lives . . . that the first thing intolerant parents often do when they find out their child is gay is ban them from the internet . . . because they realize that the internet can provide support, affirmation, and therapy."); see also Marissa Higgins, *3 Reasons We Still Need LGBTQ Safe Spaces & Why It's Important to Respect Them*, BUSTLE (Feb. 22, 2016), <http://www.bustle.com/articles/143343-3-reasons-we-still-need-lgbtq-safe-spaces-why-its-important-to-respect-them> ("Even with recent progressive legal strides in the United States, there are still people who live in the closet for fear of social repercussions or losing their employment or home. . . . For LGBTQ people, our circles are very, very limited, so when our spaces are infiltrated, it can feel like our identities are being removed.").

generally—and LGBTQ+ teens specifically—experiencing mental health issues and violence when those teens discover they are being monitored.¹²¹

A. Hindering Trust Development and Barring Effective Communication

The underlying purpose of parents using monitoring tools is safety—the ability to protect their teens by making sure they know where their teens are and who their teens are talking to.¹²² The other main justification is that monitoring allows parents to have better communication with their teen.¹²³ Between the ages of 13 and 17, the years of adolescence, it is not uncommon for teens to talk back to their parents or to stop communicating with their parents altogether.¹²⁴ Many parents worry that something is wrong with their teen, and this worry motivates the parent to get their teen talking.¹²⁵ This is especially true where teens are spending more time online and parents are concerned with cyber bullying, online predators, stalkers, etc.¹²⁶

¹²¹ See *LGBT Youth*, CENTERS FOR DISEASE CONTROL AND PREVENTION (CDC) (Nov. 12, 2014), <http://www.cdc.gov/lgbthealth/youth.htm>. Since LGBTQ+ teens already face a great risk of mental health issues, they may be more vulnerable to other constraints on their lifestyles. See *id.*

¹²² See, e.g., *Keeping Your Child Safe Using Monitoring Apps*, THEONESPY (May 21, 2015), <https://www.theonespy.com/keeping-your-child-safe-using-monitoring-apps/>.

¹²³ See Victor Luckerson, *Should You Use Your Smart Phone to Track Your Kids?*, TIME (Sept. 14, 2012), <http://business.time.com/2012/09/14/should-you-use-your-smartphone-to-track-your-kids/> (CEO of Life360 “tries to portray Life360 less as a surveillance device than as a tool for familial communication”).

¹²⁴ See Janet Lehman, *Teenagers Talking Back: How to Manage This Annoying Behavior*, EMPOWERING PARENTS, <http://www.empoweringparents.com/Teenagers-Talking-Back-How-to-Manage-It-Effectively.php> (last visited Nov. 23, 2015); see also *Help! My Teen Stopped Talking to Me*, CHILD MIND INST. (Mar. 18, 2014), <http://www.childmind.org/en/posts/articles/2014-3-18-help-my-teen-stopped-talking-me>.

¹²⁵ See user11620, *Why Would a 15 Year Old Just Stop Talking. Like ‘Selective Mutism’?*, PARENTING STACK EXCHANGE (Nov. 24, 2014), <http://parenting.stackexchange.com/questions/16695/why-would-a-15-year-old-just-stop-talking-like-selective-mutism> (“My 15 year old daughter just stopped talking and I have no clue why. She won’t talk to anybody . . . I honestly don’t know what to do about this? Can somebody please tell me what to do about this?”).

¹²⁶ Jeffrey C. Neu, *COPPA and Social Media*, 284 N.J. L. 14, 14 (2013).

However, this type of monitoring can create trust issues for the teen being monitored, especially when the teen later finds out that he or she is being monitored.¹²⁷ Several psychologists and researchers share the sentiment that parents should not be covertly monitoring their teens: “Parents should have some level of monitoring their children’s online usage but not necessarily in a covert way because that may create trust problems.”¹²⁸ Barbara Greenberg, a family clinical psychologist with an expertise in teen behavior, believes that a parent’s constant monitoring presents the message, “I don’t trust you at all.”¹²⁹ While some believe parents should not be monitoring their teens at all, others believe monitoring is okay so long as parents inform their teens they are doing so.¹³⁰ Regardless of whether the relationship between the parent and teen was good to begin with, teens are likely to feel betrayed and angered upon finding out their parents were monitoring them.¹³¹ Even authorities in other countries caution parents against using monitoring applications to track their teens’ smartphone activity, recognizing that spying applications breach trust.¹³²

Trust is important in relationships between parents and teenagers— “[w]hen teenagers feel they have the trust of their parents they are more likely to communicate openly and honestly as well as to stick to rules and

¹²⁷ IANS, *Parental Advisory! Build Trust with Kids on Internet Use*, EXPRESS TRIBUNE (Mar. 25, 2014), <http://tribune.com.pk/story/687097/parental-advisory-build-trust-with-kids-on-internet-use/>.

¹²⁸ *Id.*

¹²⁹ Grisham, *supra* note 10.

¹³⁰ See Danielle Braff, *Apps Let Parents Track Kids’ Cellphone Use*, DAILY HERALD (Aug. 18, 2015, 7:30 AM), <http://www.newsday.com/lifestyle/family/iphone-and-android-apps-to-track-kids-cellphone-use-1.10696902>.

¹³¹ See Rosalind Dorlen, *Should Parents Spy on Their Children and Teens?*, YOUR MIND YOUR BODY (June 7, 2011), <http://www.yourmindyourbody.org/should-parents-spy-on-their-children-or-teens/> (referring to parents discovering their teen is using drugs through monitoring activities, “[a]nd sometimes, the result is feelings of betrayal on both sides.”).

¹³² See, e.g., Conor Duffy & Jessicah Mendes, *Police Caution Parents Against Using New Teensafe App to Spy on Children’s Smartphone Activity*, ABC NEWS AUSTRALIA (Apr. 13, 2015, 7:35 PM), <http://www.abc.net.au/news/2015-04-13/police-caution-against-new-teensafe-spying-app-for-parents/6389660>.

parental expectations.”¹³³ For example, teens are less likely to participate in high-risk or delinquent behaviors when they feel their parents trust them.¹³⁴ Conversely, teenagers may not be as likely to communicate well with parents if there is a sense of distrust.¹³⁵

B. The Importance of Internet Access to LGBTQ+ Teens Particularly

When LGBTQ+ teens are not out to the people surrounding them, they are typically unable to communicate to those people about their sexuality related issues.¹³⁶ “LGBTQ youth, compared to youth in general, have limited use of public spaces or are limited in their expression of identity or exploration of their sexual identity in spaces such as the school environment.”¹³⁷ Therefore, LGBTQ+ teens greatly benefit from access to the Internet, which allows them to “find greater peer support, access . . . health information and [find] opportunities to be civically engaged”.¹³⁸

The Internet impacts almost all aspects of our lives, but it is particularly entrenched in the lives of youth, who are the most connected people online in our society . . . LGBT youth continue to face extraordinary obstacles in their day-to-day lives whether at school or online, but the Internet can be a valuable source of

¹³³ Victorian Dep’t of Human Services, *Trust*, ABCD PARENTING YOUNG ADOLESCENTS (2003), http://www.abcdparenting.org/index.php?option=com_jdownloads&Itemid=5&task=view.download&cid=10.

¹³⁴ *Id.*

¹³⁵ *See id.*

¹³⁶ Olu Jenzen & Irmi Karl, *Make, Share, Care: Social Media and LGBTQ Youth Engagement*, ADA: A JOURNAL OF GENDER NEW MEDIA & TECHNOLOGY, NO. 5 (2014), <http://adanewmedia.org/2014/07/issue5-jenzenkarl/>.

¹³⁷ *Id.*

¹³⁸ *Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet*, GAY, LESBIAN & STRAIGHT EDUCATION NETWORK (GLSEN) (July 10, 2013), <http://www.glsen.org/press/study-finds-lgbt-youth-face-greater-harassment-online> (quoting Dr. Eliza Byard, GLSEN’s Executive Director). Harris Interactive conducted the surveys on behalf of several organizations between August 2010 and January 2011. *Id.* This particular study was based on national surveys of 5,680 students between the ages of 13 and 18—the number of individuals identifying as LGBT in the study was 1,960. *Id.*

information and support when they have no one or nowhere else left to turn to.¹³⁹

The Harris Interactive study found that LGBTQ+ teens were more likely to be bullied or harassed than non-LGBTQ+ teens, both online and via text message.¹⁴⁰

The Harris study also showed that many LGBTQ+ teens used the Internet to cope with those negative situations.¹⁴¹ LGBTQ+ teens referred to the Internet as “a space that offers safer opportunities to express who they are.”¹⁴² The Internet is also an important source for LGBTQ+ teens to search for health and medical information that they would not be as comfortable asking about in person—81 percent of LGBTQ+ teens were likely to search for health and medical information online compared to 46 percent of non-LGBTQ+ teens.¹⁴³ Additionally, for those teens that are curious about their sexuality or are unsure about their sexual attractions, the Internet is an important resource for addressing those concerns.¹⁴⁴ Removing or limiting access to that resource could be fatal to the experiences of LGBTQ+ teens.¹⁴⁵

C. LGBTQ+ Teens and the “Coming Out” Process

In addition to the previously discussed general issues teen face from being subjected to monitoring applications and programs, LGBTQ+ teens may have a higher potential to be negatively impacted in other ways. This is

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ *See id.*

¹⁴⁴ *See id.*

¹⁴⁵ *See* Bella Qvist, *Parents, Is It OK to Spy on Your Child’s Online Search History?*, EXEC REVIEW (Nov. 5, 2015), <http://www.execreview.com/2015/11/parents-is-it-ok-to-spy-on-your-childs-online-search-history/> (“If [children] feel they are being monitored that undermines any kind of relationship of trust. They might be using the internet in a healthy way to get information and support, and feel that they are not able to do that because they are being monitored.”).

possibly attributed, in large part, to the complicated facets of staying “in the closet”¹⁴⁶ and the related “coming out” process. Many LGBTQ+ individuals stay “in the closet”; even adults choose not to disclose their sexual orientation or gender identity.¹⁴⁷ The fact that even adults are insecure about disclosing these parts of their identity suggests that teens may also be insecure as well.

LGBTQ+ teens, as opposed to teens generally, have a legitimate fear of a forced coming out resulting from parents using monitoring applications and programs.¹⁴⁸ Researchers generally estimate the LGBTQ+ community as being, at the most, ten percent of the US population.¹⁴⁹ This estimate includes both teens and adults, meaning the number of LGBTQ+ teens in the United States is less than ten percent of the population.¹⁵⁰ Yet LGBTQ+ teens comprise 20 to 40 percent of the youth homeless population, which is more than double the percentage of LGBTQ+ teens in the general population.¹⁵¹

¹⁴⁶ The term “in the closet” refers to hiding one’s sexual orientation and/or gender identity from other people. See Jarune Uwujaren, *Dealing with the Stress of Being in the Closet*, EVERYDAY FEMINISM (Nov. 18, 2013), <http://everydayfeminism.com/2013/11/the-stress-of-being-in-closet/>.

¹⁴⁷ See Pauline Anderson, *Many LGBT Medical Students Stay in the Closet*, MEDSCAPE (Feb. 28, 2015), <http://www.medscape.com/viewarticle/839934>.

¹⁴⁸ See Elizabeth Hunger, *Is the Rise of Digital Media Helping, or Hurting, Queer Youth?*, FLIP THE MEDIA (Nov. 1, 2010), <http://flipthemedias.com/2010/11/is-the-rise-of-digital-media-helping-or-hurting-queer-youth/> (“Rapinan says that numerous students have visited the Q-Center for advice after their parents or guardians began questioning the content on their Facebook pages. The proliferation of social networks has forced some queer youth to lead dual lives, monitoring every comment and “like” on their Facebook pages for fear of being inadvertently ‘outed.’”).

¹⁴⁹ Jaime Grant, *How Big is the LGBT Community? Why Can't I Find This Number?*, NATIONAL GAY AND LESBIAN TASK FORCE 2, http://www.thetaskforce.org/static_html/downloads/release_materials/tf_lgbt_community.pdf (last visited Nov. 23, 2015).

¹⁵⁰ *Id.*

¹⁵¹ Marry Cunningham et al., *Homeless LGBTQ Youth*, URBAN INST. 1 (Aug. 2014), <http://www.urban.org/sites/default/files/alfresco/publication-pdfs/413209-Homeless-LGBTQ-Youth.PDF>.

There are four categories of family relationships where a teen identifies as LGBTQ+: (1) the teen is open about his or her sexual orientation and his or her family is accepting; (2) the teen is open about his or her sexual orientation and the family relationship is strained as a result; (3) the teen is open about his or her sexual orientation, has left the home, and the family relationship is broken; and (4) the teen has not disclosed his or her sexual orientation.¹⁵² Many LGBTQ+ teens that are homeless fall within either the second or the third category, and they typically report family rejection of their sexual orientation and/or gender identity as a factor in their state of homelessness.¹⁵³

Teens are coming out at younger ages than before,¹⁵⁴ perhaps due to a slowly increasing national acceptance of LGBTQ+ individuals,¹⁵⁵ or due to teens expecting their parents and families to be accepting of them. However, about half of LGBTQ+ teens experience negative reactions upon coming out, while 26 percent are kicked out of their home.¹⁵⁶ These statistics include teens that either voluntarily came out to their parents or were forced to come out to their parents.¹⁵⁷ The latter is especially harmful due to the fact that those teens may not have been mentally or emotionally prepared to come out to their parents. LGBTQ+ teens also face higher risks of physical or sexual assault upon coming out—over a third of homeless teens and those cared for by social services experienced physical assault

¹⁵² Nicholas Ray, *Lesbian, Gay, Bisexual and Transgender Youth: An Epidemic of Homelessness*, NAT'L GAY & LESBIAN TASK FORCE 1, 17-18 (2006), http://www.thetaskforce.org/static_html/downloads/HomelessYouth.pdf.

¹⁵³ *Family Acceptance as One Solution to LGBT Youth Homelessness*, NAT'L ALLIANCE TO END HOMELESSNESS 1 (Sept. 7, 2012), <http://www.endhomelessness.org/page/-/files/Family%20Acceptance%20as%20a%20Solution%20.pdf>.

¹⁵⁴ Cunningham et al., *supra* note 151.

¹⁵⁵ See *Changing Attitudes on Gay Marriage*, PEW RES. CTR. (May 12, 2016), <http://www.pewforum.org/2016/05/12/changing-attitudes-on-gay-marriage/>.

¹⁵⁶ Ray, *supra* note 152, at 2.

¹⁵⁷ *Id.*

upon coming out.¹⁵⁸ LGBTQ teens+ are at risk of these particular consequences when parents monitor their online and mobile activity, as they may be forced into revealing their sexualities or gender identities.

D. Mental Health and Risks of Violence

Teens in general have a high risk of experiencing mental health issues, but LGBTQ+ teens are a particularly vulnerable group because of the negative stigmas surrounding LGBTQ+ individuals.¹⁵⁹ Discriminatory experiences and perceived discrimination of LGB individuals¹⁶⁰ have important mental health consequences—there is a strong relationship between ongoing discrimination against LGB individuals and issues such as anxiety or depression.¹⁶¹ LGBTQ+ teens have a higher risk of experiencing suicidal thoughts and attempting to commit suicide; in fact, LGBTQ+ teens are more than twice as likely to attempt to commit suicide than their heterosexual peers.¹⁶² In addition, LGBTQ+ teens face increased risks of violence, including behaviors bullying, harassment, physical assault, and sexual assault when they are “out.”¹⁶³ When LGBTQ+ teens already worry about facing these risks, discovering that their parents are monitoring their activity could lead to exactly the outcomes described. Even if teens know

¹⁵⁸ *Id.* at 18 (“... parents’ reactions to the discovery that a son or daughter is LGBT can lead to physical or sexual assault, and this assault can become the immediate reason for a youth becoming homeless.”).

¹⁵⁹ See *LGBT Youth*, *supra* note 121.

¹⁶⁰ LGB individuals is specifically used here the particular data from the study identifies only Lesbian, Gay, and Bisexual mental health. See *infra* note 161.

¹⁶¹ Tori DeAngelis, *New Data on Lesbian, Gay and Bisexual Mental Health*, 33 *MONITOR ON PSYCHOL.* 2, 46 (Feb. 2002), <http://www.apa.org/monitor/feb02/newdata.aspx>.

¹⁶² See *LGBT Youth*, *supra* note 121 (the rates of attempted suicide reflect that of lesbian, gay, and bisexual youth; separate studies for transgender youth reported a 25 percent rate of suicide attempts among 55 transgender youth).

¹⁶³ See *id.*

their parents are monitoring them, that knowledge may create added pressure for teens to hide their identities from their parents.¹⁶⁴

V. CURRENT LEGISLATION PROTECTING PRIVACY RIGHTS IN OTHER AREAS

Both Congress and the Washington State Legislature have passed legislation demonstrating, or at least suggesting, an intent to regulate certain types of monitoring activity.¹⁶⁵ Additionally, with the enactment of the Children's Online Privacy Protection Act, I believe Congress expressed a clear interest in protecting children's online privacy rights. The specific acts and legislation that will be discussed below include the Privacy for Consumers Workers Act (federal), the Children's Online Protection Privacy Act (federal), and the Washington Revised Code § 9.73.030 (Recording communications) (state).

A. *Privacy for Consumers and Workers Act*

Private employers experience extensive freedom in using electronic monitoring in the workplace.¹⁶⁶ The Privacy for Consumers and Workers Act (PCWA) was a bill introduced in the Senate on May 19, 1993 in response to that freedom, but the bill was not enacted.¹⁶⁷ Although the bill failed to pass the Senate, the main goal of the PCWA was to "prevent

¹⁶⁴ See John D. Sutter, *Survey: 70% of Teens Hide Online Behavior From Parents*, CNN (June 25, 2012), <http://www.cnn.com/2012/06/25/tech/web/mcafee-teen-online-survey/> ("Half of teens say they would think twice about their online activities if they knew parents were watching").

¹⁶⁵ See Health Insurance Portability and Accountability Act, Pub. L. 104-91, 110 Stat. 1936 (1996); WASH. REV. CODE § 9.73.030 (1985).

¹⁶⁶ Kristen Bell DeTienne & Richard D. Flint, *The Bosses' Eyes and Ears: The Privacy for Consumers and Workers Act*, 12 THE LABOR LAWYER 1 (1996), http://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/detienne.html; Privacy for Consumers and Workers Act, S. 984, 103rd Cong. (1993).

¹⁶⁷ S. 984, *supra* note 166.

abuses of electronic monitoring in the workplace.”¹⁶⁸ In other words, constituents were concerned that employees’ privacy interests were not being protected within the workplace. Had the bill been enacted, the PWCA would have established privacy protections against electronic monitoring by employers within the workplace while directing the Secretary of Labor to enforce those protections.¹⁶⁹ Additionally, the PCWA would have required employers to notify employees for three instances of monitoring: (1) electronic monitoring generally; (2) individual employees who would be electronically monitored, notified in writing; and (3) prospective employees who would be monitored.¹⁷⁰ Other related restrictions included how employers were allowed to use the information gathered and what information was off limits in terms of electronic monitoring.¹⁷¹

The introduction of the PCWA to the Senate demonstrated an existing concern over electronic monitoring—the drafters of the bill were aware that the type of technology allowing electronic monitoring was one that could be easily abused.¹⁷²

B. Children’s Online Privacy Protection Act (COPPA)

In 2000, Congress passed the Children’s Online Privacy Protection Act (COPPA).¹⁷³ The primary purpose of COPPA is evident in the Act’s title: to protect children’s online privacy. Specifically, COPPA gave parents a say

¹⁶⁸ *Id.*

¹⁶⁹ *Summaries for the Privacy for Consumers and Workers Act*, GOVTRACK.US, <https://www.govtrack.us/congress/bills/103/s984/summary> (last visited Nov. 23, 2015).

¹⁷⁰ DeTienne & Flint, *supra* note 166.

¹⁷¹ *Id.*

¹⁷² *See* S. 984, *supra* note 166.

¹⁷³ *FTC Strengthens Kids’ Privacy, Gives Parents Greater Control Over Their Information by Amending Childrens Online Privacy Protection Rule*, FEDERAL TRADE COMMISSION (Dec. 19, 2012), <https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over>.

in what information could be collected from their children online.¹⁷⁴ COPPA details requirements for websites and online services when their content is “directed to children under 13 years of age” or when they have actual knowledge that they are collecting personal information online from a child under 13 years of age.”¹⁷⁵ In passing COPPA, Congress delegated power to the Federal Trade Commission to issue a rule that could be enforced against websites and online services that fall within Congress’s intended categories.¹⁷⁶ One of the reasons Congress enacted COPPA was a growing concern that advertisers were gathering an increasing amount of information from children as consumers.¹⁷⁷ Tantamount to that concern were parents’ fears that advertisers and social media sites were exposing children to commercial and criminal predators.¹⁷⁸

When Congress passed COPPA, it included a qualifier that only websites or online services directed to or knowingly collecting information from *children under 13 years of age* were subject to COPPA requirements.¹⁷⁹ By Congress including this qualifier, it implied that teens that are 13 and older are not as vulnerable as children under 13 years of age. The FTC specifically states on its website that Congress recognized “younger children are particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues created by the online collection of personal information.”¹⁸⁰ Although the FTC also articulates a concern for teen privacy,¹⁸¹ the agency seems to justify Congress’s actions with

¹⁷⁴ *Complying with COPPA: Frequently Asked Questions*, FEDERAL TRADE COMMISSION (updated Mar. 20, 2015), <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>.

¹⁷⁵ *Children’s Online Privacy Protection Act (“COPPA”)*, *supra* note 2.

¹⁷⁶ *See generally id.*

¹⁷⁷ Neu, *supra* note 126, at 15.

¹⁷⁸ *Id.* at 14.

¹⁷⁹ *See Children’s Online Privacy Protection Act (“COPPA”)*, *supra* note 2.

¹⁸⁰ *Complying with COPPA: Frequently Asked Questions*, *supra* note 174.

¹⁸¹ *Id.*

language suggesting that teens, though still vulnerable, are not quite as vulnerable as children.

C. Washington's Recording Communications Statute (Wash. Rev. Code § 9.73.030)

Through enactment of a statute banning recordings of private communications, the Washington State Legislature demonstrated a need to provide privacy within private settings.¹⁸² In 1967, the legislature enacted RCW section 9.73.030 of the Washington Revised Code (“Intercepting, recording, or divulging private communication – Consent required – Exceptions”).¹⁸³ The statute made it unlawful for individuals to intercept or record private communications¹⁸⁴ or private conversations¹⁸⁵ without getting the consent of all individuals that were party to the communication or conversation.¹⁸⁶ There is no language in the statute suggesting the legislature intended to limit the statute’s provisions to specific age groups.¹⁸⁷ The legislature used phrases such as “[private communication . . . between two or more individuals . . .]”¹⁸⁸ and “. . . obtaining the consent of all the persons engaged in the conversation.”¹⁸⁹ The use of these general terms places significance on the people involved in the conversations, rather than who the parties actually are (i.e. the relationship they have to one another).

Additionally, chapter 9.73 contains exceptions for certain individuals or entities the legislature believed should be able to intercept private

¹⁸² See generally WASH. REV. CODE § 9.73.030 (1986).

¹⁸³ *Id.*

¹⁸⁴ WASH. REV. CODE § 9.73.030(a) (1986) (private communications include those “transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic”).

¹⁸⁵ *Id.* (“by any device electronic or otherwise designed to record or transmit such conversation”).

¹⁸⁶ WASH. REV. CODE § 9.73.030(1)(a) (1986).

¹⁸⁷ See WASH. REV. CODE § 9.73.030 (1986).

¹⁸⁸ WASH. REV. CODE § 9.73.030(1)(a) (1986).

¹⁸⁹ WASH. REV. CODE § 9.73.030(1)(b) (1986).

communications or conversations under certain circumstances.¹⁹⁰ Examples of such individuals include building owners when persons involved in the communication or conversation are engaged in a criminal act or 911 emergency services.¹⁹¹ Had the legislature intended to exclude parental interception or recording of private communications or conversations, it likely would have included it as an exception to the statute. Application of the statute to teens and the recording of teens' private communications will be further discussed in the section below.

VI. THREE-PART SUGGESTION FOR TWO-PARTY CONSENT REQUIREMENT BEFORE PARENTS USE MONITORING TOOLS ON TEENS

The Washington State Legislature should undertake the following three suggestions to balance the need for teen privacy rights with the need to protect teens from outside harm: (1) extend the scope of Washington's two-party consent requirement for the electronic communications section of the Washington Privacy Act¹⁹² to include parents' use of monitoring tools, (2) apply the "announcement" standard¹⁹³ for consent in the electronic communications section to the process for obtaining consent from parties that are not the parents' own teen, and (3) require monitoring tool distributors to ensure two-party consent is achieved before use by establishing new legislation outlining the specific requirements for monitoring tool distributors to abide by, including minimum recordkeeping standards. Through the implementation of these three suggestions, parents will be allowed to continue using monitoring tools to observe their teens.

¹⁹⁰ See WASH. REV. CODE, tit. 9, ch. 9.73; *see, e.g.*, WASH. REV. CODE § 9.73.070 (1994); WASH. REV. CODE § 9.73.090 (2011); WASH. REV. CODE § 9.73.110 (1977).

¹⁹¹ WASH. REV. CODE § 9.73.070(2)(b) (2011); WASH. REV. CODE § 9.73.110 (1977).

¹⁹² WASH. REV. CODE § 9.73.030(1) (1986).

¹⁹³ WASH. REV. CODE § 9.73.030(3) (1986) (the announcement standard is that the recording party must disclose to all parties to the conversation that communication is being recorded).

However, these suggestions circumvent the possibility of parents doing so covertly. Thus, parents may protect their teens from outside harm while still affording their teens some level of privacy.

A. Extending Scope of Two-Party Consent to Monitoring Tools

The Washington State Legislature likely anticipated the extension of the “wiretapping law” to newer advancements in communication recording technology when it used the words “[p]rivate communication . . . between two or more individuals . . . by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated . . .”¹⁹⁴ The legislature originally amended the Privacy Act to include the electronic communications section during a time when people were inventing new methods of recording communications¹⁹⁵ such as the audio cassette tape¹⁹⁶ and optical-digital recording.¹⁹⁷ The legislature’s use of broad language seems to encompass any communication technologies that the legislature was either unaware of or could appear after the statute’s enactment. Although the legislature could have amended the statute to list specific communication technologies, it chose to leave the language broad enough to apply to new or undiscovered technologies.¹⁹⁸ Because the language covers newer communication technologies, the

¹⁹⁴ *Id.* at (1)(a).

¹⁹⁵ The legislature added the electronic communications section (WASH. REV. CODE § 9.73.030) to the Privacy Act in 1967.

¹⁹⁶ *A History of the Cassette Tape and Deck*, EBAY (June 9, 2014), <http://www.ebay.com/gds/A-History-of-the-Cassette-Tape-and-Deck-/10000000177628959/g.html> (Phillips introduced the compact cassette in 1962).

¹⁹⁷ Brier Dudley, *Scientist's Invention Was Let Go for a Song*, SEATTLE TIMES (Nov. 29, 2004, 12:35 PM), http://old.seattletimes.com/html/business/technology/2002103322_cdman29.html (Jim Russell developed the underlying technologies for compact discs (CDs) and digital versatile discs (DVDs) in 1965).

¹⁹⁸ See WASH. REV. CODE § 9.73.030 (1986) (the legislature amended the statute three times—in 1977, 1985, and 1986—but the language regarding the communication technologies remained).

provisions of the Privacy Act should also apply to communications made through mobile phones and other similar devices.

Specifically, the Privacy Act's two-party consent requirement should be applied to mobile phone and mobile device communications. To intercept or record private communications or conversations made through a device, Washington law requires the recorder obtain the consent of all the communicating or conversing parties (minimum of two).¹⁹⁹ Although methods of conversing, such as texting and instant messaging are done through mobile devices, parents using monitoring tools are not required to obtain the consent of either their teen or the individual their teen is conversing with.²⁰⁰ This lack of application to parents and their monitoring of teens' mobile devices would read an exception into the statute that has not yet been recognized.

While the Privacy Act contains exceptions for emergencies and other unreasonable communications, it does not contain exceptions for instances of parental monitoring or parental use of monitoring tools.²⁰¹ In fact, the Washington Supreme Court explicitly rejected recognizing a parental exception to the privacy act's "all-party consent requirement."²⁰² The case

¹⁹⁹ WASH. REV. CODE § 9.73.030(1) (1986).

²⁰⁰ See *Frequently Asked Questions*, TEENSAFE, <http://www.teensafe.com/> (last visited Feb. 10, 2016) ("Many parents choose to tell their teen that they're using TeenSafe. This choice is, however, entirely up to the discretion of the parent.").

²⁰¹ WASH. REV. CODE § 9.73.030(2) (1986) ("Notwithstanding subsection (1) of this section, wire communications or conversations (a) of an emergency nature, such as the reporting of a fire, medical emergency, crime, or disaster, or (b) which convey threats of extortion, blackmail, bodily harm, or other unlawful requests or demands, or (c) which occur anonymously or repeatedly or at an extremely inconvenient hour, or (d) which relate to communications by a hostage holder or barricaded person as defined in RCW 70.85.100, whether or not conversation ensues, may be recorded with the consent of one party to the conversation."); WASH. REV. CODE § 9.73.070 (1986) (persons and activities excepted from Privacy Act chapter does not include parents or parental monitoring).

²⁰² *State v. Christensen*, 153 Wash. 2d 186, 193-94, 102 P.3d 789 (2004) (en banc) ("The federal wiretap statute . . . has been interpreted to permit parents acting to protect the welfare of a child, to consent vicariously for their child to the recording of their child's conversations. [citations omitted] The Washington act, with its all-party consent

involved a 17-year-old defendant suspected of a robbery.²⁰³ The sheriff informed the defendant's minor-girlfriend's mother to keep a lookout for any evidence that could surface.²⁰⁴ When the defendant later telephoned his girlfriend, her mother used the speakerphone function on the cordless telephone system to listen to their conversation.²⁰⁵ The defendant confided in his girlfriend that he was aware of the police's suspicions and knew where the stolen items are.²⁰⁶ Neither the defendant nor his girlfriend knew of or consented to the mother listening to the conversation.²⁰⁷ The court held the communication was private,²⁰⁸ even though it was between minors, and that admitting the mother's testimony of what was heard through the speakerphone was erroneous.²⁰⁹ Acknowledging that the legislature passed the electronic communications portion of the Privacy Act²¹⁰ before the development of mobile phones, the court found the "base unit of a cordless telephone system" falls within the meaning of "device designed to transmit."²¹¹ It sought to interpret the language of the Privacy Act "in a manner that ensures that the private conversations of this state's residents are protected in the face of an ever-changing technological landscape."²¹² Thus, the Washington Supreme Court has recognized two points supporting the application of Washington's Privacy Act to parental use of monitoring tools: (1) the language of the Privacy Act should be interpreted to maintain individual's privacy rights in communications and conversations in the face

requirement, contains no such parental exception and no Washington court has ever implied such an exception. We decline to do so now.").

²⁰³ *Id.* at 190.

²⁰⁴ *Id.*

²⁰⁵ *Id.*

²⁰⁶ *Id.* at 190-91.

²⁰⁷ *Id.* at 191.

²⁰⁸ *Id.* at 192-94 (the court may decide whether a particular communication is private as a question of law if there are no disputed facts).

²⁰⁹ *Id.* at 200-01.

²¹⁰ WASH. REV. CODE § 9.73.030 (1986).

²¹¹ Christensen, 153 Wash. 2d at 194-200.

²¹² *Id.* at 197.

of new technologies;²¹³ and (2) parental monitoring is not an exception to the provisions of the Privacy Act.²¹⁴

Since the legislature’s language remains broad and the Washington Supreme Court has interpreted the legislature’s language to apply to parent-minor situations, the legislature should extend the scope of the two-party consent requirement to parental use of monitoring tools. Although not otherwise mentioned in this article, it might be beneficial for these requirements to apply to parties who are not the teen’s parent or guardian. While the intent is to protect teens against parents monitoring their teens’ activities without the teens’ consent, there is also an interest in protecting teens from other adult family members monitoring the teens’ activities (e.g. uncles and aunts who are not the teens’ legal guardians).²¹⁵ It is likely that the two-party consent requirement already applies to this group of people since there is no statutory exception for family members.²¹⁶

B. Applying the “Announcement” Consent Requirement to Monitoring Tools

If the legislature applies the “announcement” consent standard to monitoring tools, it will address the issue of requiring a party other than the monitoring parent’s child to also consent to the communication. Since the Privacy Act requires consent from all parties,²¹⁷ the other party to the

²¹³ *Id.*

²¹⁴ *Id.* at 193-94. The court additionally found it did not matter that the mother had eavesdropped on the girlfriend’s conversations before since neither the defendant nor the girlfriend was aware of the mother’s prior monitoring.

²¹⁵ See *Three Reasons To Not Teach Body Safety to Kids*, THE MAMA BEAR EFFECT (Sept. 13, 2015), <http://themamabeareffect.org/blog/three-reasons-to-not-teach-body-safety-to-kids> (acknowledging that most cases of child sexual abuse involved a family member or someone close to the family); see also *Predators Within The Family*, THE MAMA BEAR EFFECT (June 15, 2015), <http://themamabeareffect.org/1/post/2015/06/predators-within-the-family.html> (discussing how to keep kids safe from the people we know and trust).

²¹⁶ See WASH. REV. CODE § 9.73.030 (1985).

²¹⁷ WASH. REV. CODE § 9.73.030(1) (1986).

communication should not be overlooked. The major issue with extending the scope of the two-party consent requirement to parents' use of monitoring tools as currently written in the statute is the exclusion of consent required from the other party to the communication.

By applying the "announcement" consent standard, the consent of the other party to the communication would effectively be obtained. The "announcement" consent standard of the electronic communications privacy act provision states:

. . . consent shall be considered obtained whenever one party has announced to all other parties engaged in the communication or conversation, in any reasonably effective manner, that such communication or conversation is about to be recorded or transmitted: PROVIDED, That if the conversation is to be recorded that said announcement shall also be recorded.²¹⁸

The standard effectuates consent when the announcement is made to all parties that a particular communication or conversation will be recorded or transmitted so long as the announcement is made in a reasonable manner.²¹⁹

In the parental monitoring context, this could include parents texting their teens or verbally communicating to inform the teens they are monitoring the teens' mobile phone communications.²²⁰ Additionally, parents could also text or verbally communicate with the people their teens are communicating with to announce they are monitoring their teens' communications, as well as the third party's messages to the parents' teens.²²¹

However, applying the "announcement" consent standard should not be a substitute for the two-party consent requirement as applied to parents and

²¹⁸ WASH. REV. CODE § 9.73.030(3) (1986).

²¹⁹ *Id.*

²²⁰ See *5 Ways To Tell Your Teen You're Using a Mobile Spy*, TEENSAFE (Apr. 24, 2015), <http://www.teensafe.com/blog/5-ways-to-tell-your-teen-youre-using-a-mobile-spy/> (encouraging parents to talk to their teens about their use of monitoring tools).

²²¹ See *id.* The same concepts surrounding parents talking to their own teens could apply to talking to their teens' friends about why they feel they need to monitor their teens' communications.

their teen(s). The suggestion to apply the “announcement” consent standard is meant to address the gap in protecting third parties left by applying the two-party consent requirement. On the other hand, the suggestion to apply the two-party consent requirement is meant to maximize teen privacy in relation to protecting teens. While the “announcement” consent standard addresses the disclosure issue for all parties involved, it lacks the affirmative consent aspect of the two-party consent requirement.

C. Requiring Monitoring Tool Distributors to Monitor Consent and Creating Standards Through Legislation

Since the “announcement” consent standard should not be substituted the two-party consent requirement, the legislature should create a new standard addressing how to satisfy consent for use of parental monitoring. Currently, the Washington Privacy Act contains statutes outlining the requirements for obtaining authorization to record private communications.²²² However, those statutes do not address how parents would obtain consent from their teens²²³ and the current outlined requirements may not fit the parental monitoring context. Therefore, the legislature should create a consent requirement specifically tailored to parental monitoring. This new consent requirement should further describe who is required to monitor consent in order to ensure accountability for any lack of consent.

Objectively speaking, the party that is likely in the best position to monitor whether parents have obtained consent is the distributor of the monitoring tool the parents seek to use. Rather than a parent being responsible for ensuring they obtain consent from their teen, it may be more reasonable for the distributor of the monitoring tool to ensure that both the parent and teen consent or act as witness to the process.²²⁴ Not only does

²²² WASH. REV. CODE §§ 9.73.130-140 (2011) (outlining requirements for applying for authorization to record private communications of criminal suspects).

²²³ See *id.*

²²⁴ See *A Guide to Informed Consent – Information Sheet*, U.S. FOOD AND DRUG ADMIN. (FDA), <http://www.fda.gov/RegulatoryInformation/Guidances/ucm126431.htm> (last

this allow for an objective third party to oversee the consent process, it also creates accountability when consent is not obtained. If the legislature requires monitoring distributors to require and keep records of consent, a court will be able to question the distributors if two-party consent is not found. Furthermore, distributors could be held directly accountable if parents are using the distributors' monitoring tools without their teen's consent.²²⁵ Since the monitoring tool distributors are an objective third party to the parent and teen consent process and could be held directly accountable, the legislature should require monitoring tool distributors to oversee two-party consent prior to parents' use of the tool.

D. What the Consent Requirements Should Look Like

The consent process between the parents and the teens needs to consider that parents will seek to use and install the monitoring tools at any point in their teens' mobile phone "ownership,"²²⁶ and not just when they first purchase the phone.²²⁷ Thus, any consent process must be applicable at any point during the teens' mobile phone ownership. However, the consent

updated Jan. 25, 2016) (finding the use of an impartial witness to observe the process of informed consent in certain medical situations). The fact that impartial witnesses are sometimes recommended where forms of consent are involved highlights the benefits of an objective party in monitoring consent.

²²⁵ Certain distributors, such as TeenSafe, indicate in the "Terms of Use" that parents may not use the tools in violation of any State or local laws, rules, ordinances, or governmental regulation. *See* TEENSAFE, *supra* note 66. Legislation that would require the monitoring of two-party consent would create a violation where the tool was being used without the requisite consent.

²²⁶ Since the parent is typically the one who purchases the mobile phone, the parent is considered the "owner" of the mobile phone. *See* Zack Whittaker, Jason Perlow & Charlie Osborne, *Should Parents Spy on Their Kids?*, ZDNET (Oct. 14, 2013), <http://www.zdnet.com/article/should-parents-spy-on-their-kids/> (In the rebuttal section, Perlow states, "Parents raising their children are analogous to being their own government in many respects, and they set the rules and laws by which their children must obey.").

²²⁷ *See All Inclusive Mobile Phone Monitoring*, MOBILE SPY, <http://www.mobile-spy.com/mobile-phone-monitoring.html> (last visited Feb. 10, 2016) (stating that Mobile Spy is easy to set up "[w]hen you're ready to start monitoring your child . . .").

process must be completed prior to installing the monitoring tool on the teen's mobile phone. Allowing installation and use prior to completing the consent process would neutralize the effects of any of the actions suggested in this article. Additionally, parents that were using monitoring tools prior to the enacted legislation would also be required to go through the consent process. Thus, the legislation would apply both past and future parental use of monitoring tools.

1. Age Specifications

Teens between 13 and 17 years of age should be protected by a two-party consent requirement for parental use of monitoring tools. COPPA's requirements protect children less than 13 years of age, implying that teens 13 years of age and above retain some type of personal autonomy regarding what they are able to access on the internet.²²⁸ Furthermore, the period between 13 and 17 years old is when teens often experience the most rapid development, both mentally and physically.²²⁹ It is during this time teens need privacy in their lives in order to cope with the changes they are experiencing.²³⁰ The FTC would potentially support such requirements for this particular age group considering that it has stated an interest in regulations for teen privacy in relation to COPPA.²³¹

2. Format for the Two-Party Consent Process

Although there are multiple formats by which a consent process for parental monitoring could potentially work, the methods discussed here

²²⁸ This excludes sexually explicit material, which is limited to individuals who are 18 years of age or older.

²²⁹ See *The Growing Child: Adolescent (13 to 18 Years)*, STANFORD CHILDREN'S HEALTH, <http://www.stanfordchildrens.org/en/topic/default?id=the-growing-child-adolescent-13-to-18-years-90-P02175> (last visited Nov. 23, 2015).

²³⁰ See *Stages of Adolescence*, AM. ACAD. OF PEDIATRICS, <https://www.healthychildren.org/English/ages-stages/teen/pages/Stages-of-Adolescence.aspx> (last updated Nov. 21, 2015) (discussing the confusing and conflicting nature of navigating the adolescence state of development).

²³¹ *Complying with COPPA: Frequently Asked Questions*, *supra* note 174.

attempt to ensure that two-party consent is actually achieved and requires the same type of form or application. First, the consent process could be done through filling out a paper application and sending it to the monitoring tool distributor through mail or fax. Alternatively, the consent process could be done through an appointment with all relevant parties, including the parent, the teen, and a representative of the monitoring tool distributor. The alternative method could involve a paper application or an electronic version with the distributor representative recording the parents' and teens' responses. The main reason to not provide an at-home electronic method is to circumvent the possibility of parents filling out and signing applications for their teens. Since the purpose of introducing these methods is to ensure two-party consent is achieved, the possibility of parents unilaterally signing applications for both parties suggests an electronic method should not be used unless a distributor representative is present. Of the two methods introduced, the physical appointment is preferred because it covers the issues presented by the at-home electronic method and involves the distributor in the process to a greater extent than simply processing a paper form application.

Due to the proposed contents of the application, both methods require the parents to sit down with their teens and review the application together. The language of the legislation should require any applications to consist of the general identification information found on most forms, including the names of the consenting parties, dates of birth, age, gender, address, phone number, etc. While the contents of consent applications for parental use of monitoring tools would need to contain the general information, each distributor should tailor its application to identify the specific services and/or features its tool offers for users.²³² However, the legislation should further require distributors to include any and all services they offer on the

²³² All monitoring tools do not provide monitoring for the same applications; additionally, tools often do not offer the same features for iPhones and Androids.

application, as well as descriptions of particular applications the tool purports to monitor. For example, if TeenSafe claims to allow parents to have access to Instagram, it must provide a description of what Instagram is as well as information regarding what is required to access the teen's Instagram.²³³ Going through a list of available applications the parent can monitor allows for transparency between the parent and teen—the parent alerts the teen to what applications he or she wants to monitor, while the teen has full knowledge that the parent will be monitoring those specific applications. Through the signatures of the parent and the teen, both parties would acknowledge their consent to the parents' use of the monitoring tool.

3. Eliminating the Covert Aspect of Monitoring Tools

Since the discussed consent processes provide a high level of transparency regarding parental use of monitoring tools, the legislature should further require distributors to make the tool visible on the teen's mobile phone. Some monitoring tools are currently meant to be covert; therefore, when parents install them, the application icon is not visible on the teen's mobile phone.²³⁴ Where the main purpose of enforcing the consent requirement through the proposed consent processes is to make the teen aware of the monitoring, the reason for the covert aspect of the monitoring tools is eliminated. Thus, if the covert aspect is no longer necessary, the legislature should ensure that distributors are not able to make their monitoring tools run covertly on mobile phones.

²³³ For social media applications, the parent generally needs to have the login information for the teen's account before the parent may monitor the particular social media account. See *Monitor Your Child's iMessages with TeenSafe*, BE WEB SMART, <http://www.bewebsmart.com/parental-controls/monitor-imessage-with-teensafe/> (last modified Nov. 2, 2015) ("And you'll also need your child's Instagram username and password.").

²³⁴ See *How Does TeenSafe Work With IOS Devices (iPhone, iPod, iPad)?*, TEENSAFE, <https://teensafe.zendesk.com/hc/en-us/articles/201811985-How-does-TeenSafe-work-with-iOS-devices-iPhone-iPod-iPad-> (last visited Aug. 4, 2016) ("No mobile apps, products or TeenSafe logos will show up on your child's iPhone.").

4. Recordkeeping Requirements for Monitoring Tool Distributors

Because implementing the discussed consent processes would require monitoring tool distributors to receive some sort of application, the legislature should further require distributors to maintain records of those applications. Once a parent and teen submit an application, using either of the two discussed methods, the distributors should have full discretion whether to accept or reject the application. If the legislature requires distributors to maintain application records, distributors will have an easier time identifying families who re-apply and have previously been rejected or families who re-apply and have been previously accepted for another teen's mobile phone. Distributors will also be able to easily identify whether a parent or another adult family member using the monitoring tool has not obtained consent prior to use.

VII. ARGUMENTS OPPOSING A TWO-PARTY CONSENT REQUIREMENT

When parents use discrete monitoring tools without obtaining their teens' consent, they emphasize a general belief that it is okay for them to monitor activity covertly.²³⁵ User reviews suggest an overall appreciation for the creation of monitoring tools and the usefulness of the tools in tracking their teens.²³⁶ As has been touched on previously, parents and supporters of monitoring activity justify their beliefs using a variety of different reasons such as (1) the "parents' rights" argument, and (2) the need to protect their teens.

²³⁵ See Michelle Charlesworth, *'Teen Safe' App Lets Parents Keep Track of Their Kids Texts and Posts*, ABC7NY EYEWITNESS NEWS (Sept. 23, 2014), <http://abc7ny.com/family/spying-or-good-parenting-new-app-helps-parents-track-their-kids/321091/> (the creator of TeenSafe distinguishes "spying" from "loving parenting").

²³⁶ See Brian S. Hall, *Best Parental-Control Apps 2015*, TOM'S GUIDE (Apr. 17, 2015), <http://www.tomsguide.com/us/best-parental-control-apps,review-2258.html> (compiling a list of the best parental control applications).

A. The “Parents’ Rights” Argument

Since courts and the government have recognized parents as being in the most favorable position to take care of and raise their children, those institutions generally tend to respect privacy within the home.²³⁷ As such, parents are essentially afforded the “right to be a parent” and protect their children with their own methods.²³⁸ However, even within the home, there are certain illegal activities that occur, such as rape, sexual assault, physical abuse, and verbal abuse. The discretion of parents in how they raise their teens is not necessarily a free pass to do whatever they like.²³⁹

First, when parents monitor their teens’ private communications with other individuals, they are necessarily invading the privacy of the individuals the teen is conversing with.²⁴⁰ Since monitoring applications and programs allow parents to view sent as well as received messages from different messaging platforms, they are reading not only their teens’ private messages, but also the other party’s private messages.²⁴¹ In the same way a parent would not be allowed to monitor a random stranger’s messages, the same idea should apply to the individual a parent’s teen is communicating with, since that person is effectively a stranger to the parent.²⁴²

²³⁷ See Shmueli & Blecher-Prigat, *supra* note 7, at 761.

²³⁸ See *id.* at 761-62.

²³⁹ See Jayne Cravens, *A Teenager’s Guide to Emancipation*, <http://www.coyotecommunications.com/stuff/emancipate.shtml> (last visited Feb. 10, 2016) (if a teenager can convince a court that independence from his or her parents is in his or her best interest, the court will grant emancipation; this could potentially result from bad parenting); see also *Reunifying Families*, CHILD WELFARE INFORMATION GATEWAY, <https://www.childwelfare.gov/topics/permanency/reunification/> (last visited Feb. 10, 2016) (acknowledging that some “children must be removed from their families to ensure their safety”).

²⁴⁰ See WASH. REV. CODE § 9.73.030(3) (1986) (where consent from all parties is needed to record electronic communications, parents overlook the party communicating with their teen by not announcing their monitoring to that party).

²⁴¹ TEENSAFE, <http://www.teensafe.com/> (last visited Feb. 10, 2016) (TeenSafe allows users to “[v]iew sent, received and deleted SMS and iMessages”).

²⁴² See *id.* (under this statute, recording a stranger’s electronic communications is illegal).

Second, the Washington Supreme Court has explicitly recognized a greater need for teen privacy.²⁴³ Washington's Privacy Act imposes stricter requirements on those intercepting or recording private electronic communications than the federal wiretap act does.²⁴⁴ Yet the Washington Supreme Court refused to read into the statute an exception for vicarious parental consent when the parent is acting to protect the welfare of the child,²⁴⁵ demonstrating the intent of the court to extend protections for teens' telephonic or electronic communications even within the home.

B. Preserving Teen Privacy versus Protecting Our Teens

The most prominent argument for allowing undisclosed monitoring of teens is the general concern in keeping teens safe.²⁴⁶ Because teens have such expansive access to the internet and social media platforms, parents fear their teens have a higher risk of being exposed to unfavorable contact and of soliciting unwanted contacts from third parties who have the intention of harming them.²⁴⁷ However, psychologist Sue Firth contends, "tracking is more about assuaging the parent's anxieties than the child's. Sadly, rare though these incidents are, no monitoring tool can prevent a child being stabbed just around the corner from their school."²⁴⁸ To some degree, Ms. Firth may be right in that no matter how much a parent monitors their teen, there are some occurrences parents are unable to prevent. Simply because a parent knows what is bothering their teen

²⁴³ Christensen, 153 Wash.2d at 199.

²⁴⁴ Compare 18 U.S.C. § 2511(2)(c) (allowing lawful interception where an individual is party to the communication or where consent is obtained from one party to the communication), with WASH. REV. CODE § 9.73.030(1) (1986) (requiring consent from all parties to a communication).

²⁴⁵ How the federal statute is interpreted.

²⁴⁶ See Helen Carroll, *Mothers Who Spy on Their Child's Every Move: A New Phone App Makes Keeping Track of Your Offspring Easy, but Will It Backfire?*, DAILYMAIL.COM (Feb. 12, 2015, 6:47 PM) ("... I've always lived in fear of my children being abducted . . .").

²⁴⁷ See *id.*

²⁴⁸ *Id.*

because they viewed the teen's messages does not necessarily mean the teen is going to discuss it with the parent, even more so if the teen discovers the parent got that information by monitoring the teen.²⁴⁹ Furthermore, relying on monitoring tools to determine whether teens are safe runs the risk of frustrating the parent if the application or program posts inaccurate information.²⁵⁰ Location tracking is not infallible and may cause parents unnecessary stress when they discover their teen is not where he or she should be.²⁵¹

Additionally, if the purpose of monitoring teens is to protect them, covertly monitoring teens may not serve that purpose and could potentially end up harming teens. Particularly with the high risk LGBTQ+ teens face towards being rejected by their families,²⁵² the harms resulting from monitoring may outweigh the benefits. At some point, a parent may successfully prevent their teen from talking to someone they do not approve of or from partaking in activities they prohibit, even when these people or activities may actually be beneficial to the teen. However, if a parent discovers their teen's sexual orientation and/or sexual identity and disapproves of that as well, then the original purpose of protecting the teen is negated. Considering that a large portion of LGBTQ+ teens who are homeless cite to family disapproval as the leading factor in their homelessness,²⁵³ the potential for forcing teens to come out through monitoring their activity is overall a path society should not endorse.

²⁴⁹ See Tim Lott, *You Can't Force a Teenager to Talk to You*, THE GUARDIAN (May 30, 2014), <http://www.theguardian.com/lifeandstyle/2014/may/30/cant-force-teenager-talk> (discussing reasons why teens do not talk to their parents even when parents initiate the talk).

²⁵⁰ See *Life360 reviews*, SITEJABBER, <http://www.sitejabber.com/reviews/www.life360.com> (last visited Feb. 10, 2016) (showing user reviews for Life360 expressing frustration with the inaccuracy of pinpointing location).

²⁵¹ *Id.*

²⁵² Ray, *supra* note 152, at 2.

²⁵³ *Id.*

However, there are legitimate uses for monitoring teens where parents may have a reasonable belief that they should be concerned.²⁵⁴ Tracking a teen's location may make it less likely that teens will be kidnapped without the parents knowing.²⁵⁵ Viewing their teen's messages may be acceptable if parents obtain their teen's consent because they believe their teen is depressed and having suicidal thoughts.²⁵⁶ Additionally, parents in many high profile cases of school shootings or mass killings committed by teens are often criticized for not seeing the warning signs.²⁵⁷ In those types of cases, where the parent has a reasonable belief that their teen may harm themselves or others, viewing their messages could be justified; however, even in situations where this is justified, parents should still be required to obtain consent to balance the teen's privacy needs.

VIII. CONCLUSION

To address the lack of legislation and regulation surrounding teen cyber privacy, the Washington State Legislature should adopt the suggestions laid out in Section V by (1) extending the scope of Washington's two-party consent requirement for the electronic communications section of the Washington Privacy Act to include parents' use of monitoring tools, (2) applying the "announcement" standard for consent in the electronic communications section to obtaining consent for parties that are not the parents' own teen, and (3) requiring monitoring tool distributors to ensure two-party consent is achieved before use by establishing new legislation

²⁵⁴ See Charlesworth, *supra* note 235 (the creator of TeenSafe shares that she discovered her teen was using and selling drugs by using the monitoring application.).

²⁵⁵ See Larry Magid, *Can GPS Prevent Abductions?*, CBS NEWS (Sept. 1, 2009, 6:45 AM), <http://www.cbsnews.com/news/can-gps-prevent-child-abductions/> (discussing the benefits of using GPS technology to prevent abductions).

²⁵⁶ See *How To Prevent Teen Suicide with Cell Phone Spying Software*, WEEBLY (June 2, 2015), <http://www.cbsnews.com/news/can-gps-prevent-child-abductions/>.

²⁵⁷ See Kelly Wallace, *After Mass Shootings, Do Parents Shoulder Some of the Blame?*, CNN (Oct. 7, 2015, 5:58 PM), <http://www.cnn.com/2015/10/07/health/oregon-shooting-parents-blame/>.

outlining the specific requirements for monitoring tool distributors to abide by, including minimum recordkeeping standards. American adults express the opinion that they do not want to be observed without their approval,²⁵⁸ yet overlook that consideration for teens through justifications such as wanting to keep teens safe or wanting to know what is going on in their teens' lives. While there is nothing wrong with parents wanting to be part of their teens' lives, monitoring their activity without their teens' consent could essentially do more harm than good, to both the teen and to the parent-teen relationship. Considering the higher risk of danger LGBTQ+ teens are exposed to when parents monitor their activity, the legislature should require two-party consent prior to parental use of monitoring tools such as applications and software designed to monitor mobile phone or computer activity. The legislature should aim to protect teens aged 13 years old to 17 years old from this type of monitoring behavior. Adopting these suggestions would allow for the legislature to balance teens' need for privacy with parents' need to protect their teens.

²⁵⁸ Maddie & Rainie, *supra* note 3.