I. Introduction

Adoption was not known at common law, and sealing adoption records and birth certificates to deny adult adoptees access to their own birth records was not common in the United States until the second half of the twentieth century. Since that time, while a growing number of states have enacted statutes allowing at least some adult adoptees to have access to their original birth or adoption records, either on an absolute basis or in the absence of a veto by the birth parent, most states still maintain sealed records for all or most adoptees. Although courts may have the authority to unseal records “for good cause shown,” they rarely do, and appellate courts rarely overturn denials, often citing the privacy rights of the birth parents and even the adoptive parents. In the twenty-first century, adoptions are no longer clothed in the secrecy that typified the mid-twentieth century. According to one study, closed infant adoptions in the United States now account for only about 5% of adoptions.

Private and state-run mutual consent registries may allow some adoptees and their birth parents or siblings to connect with one another, but such registries require both parties to sign up on the same registry, and sometimes require paying a fee. Some states have confidential intermediary programs to make connections where the parties agree. Some people hire private investigators to conduct their searches using databases not available to the general public.

However, many adoptees and birth parents use social media to make their connections, find information, create family trees, and stay in touch. They may do so to save money or time, or to eliminate the need to go through intermediaries to gain knowledge about their own families. As people have become more familiar with the Internet and more comfortable using social media, tapping these resources to get around the sealed records laws is a choice many make. Ultimately, Internet resources may make the remaining sealed records laws largely ineffective. This self-help through social media can be very effective, but there remain many social and legal questions about the privacy rights of all parties involved and whether such use exposes the searcher to legal liability.

There are few, if any, reported decisions which directly address the legal propriety of using social media for such purposes. Part II discusses sealed records and privacy issues in adoption. Part III discusses uses of social media by adoptees, birth parents, and other birth family members to find information about one another and to stay in touch. Part IV discusses privacy issues in social media. Part V addresses the social and emotional ramifications of connecting through social media. Part VI discusses potential legal liability issues arising from the use of social media in post-adoption search and reunion and the potential impact of such searches on other members of the birth and adoptive families. Finally, Part VII suggests that the adoptee and birth family share a history, and that each has the right to explore and communicate that history without being found to have abridged the privacy of the other.
II. Sealed Records and Privacy

The majority of state laws that explicitly allow adult adoptees to access their original birth certificates have been upheld. Oregon passed an initiative, Measure 58, permitting adoptees over the age of twenty-one to have access to their original birth records and thus to learn the identities of their birth mothers. Seven birth mothers who had placed their children for adoption between the years 1960 and 1994 sought declaratory and injunctive relief to prevent disclosure of their children's original birth certificates. The mothers claimed that the initiative violated the contracts clause of the state and federal constitutions and unconstitutionally violated their state and federal constitutional rights to privacy. The trial court denied their claim on summary judgment, granting the State's motion for summary judgment, and the Oregon Court of Appeals upheld the ruling in Does 1, 2, 3, 4, 5, 6, and 7 v. State. The court found:

At no time in Oregon's history have the adoption laws prevented all dissemination of information concerning the identities of birth mothers. At no time in Oregon's history have the adoption laws required the consent of, or even notice to, a birth mother on the opening of adoption records or sealed birth certificates. Moreover, the laws do not demonstrate a legislative intent to elevate considerations of a birth mother's desire for confidentiality over the legitimate needs of other interested parties in obtaining information concerning the birth. Therefore, the court found that Measure 58 does not impair any contractual rights.

More pertinent to the discussion is the court's holding regarding the asserted privacy rights of the birth mothers. The court rejected the idea “that the framers of the Oregon Constitution intended to confer on birth mothers a constitutional right to conceal their identities from their children.” Instead, the court held:

Those provisions, taken separately or together, have never been construed as providing a general privacy right under the Oregon Constitution. As noted above, adoption was unknown at common law, and early adoption statutes made no provisions for protecting the identities of birth mothers.

The court noted that “[a]doption necessarily involves a child that already has been born, and a birth is, and historically has been, essentially a public event.”

In Humphers v. First Interstate Bank of Oregon, the Oregon Supreme Court found no tortious breach of privacy where a physician assisted an adoptee in obtaining identifying information about herself from medical records. The court recognized the need to balance the rights of the birth mother and of the adoptee, stating:

[A] daughter's interest in her personal identity here confronts a mother's interest in guarding her own present identity by concealing their joint past. But recognition of an interest or value deserving protection states only half a case. Tort liability depends on the defendant's wrong as well as on the plaintiff's interest, or “right,” unless some rule imposes strict liability. One's preferred seclusion or anonymity may be lost in many ways; the question remains who is legally bound to protect those interests at the risk of liability.

The court further noted, “Nor, we think, would anyone who knew the facts without an obligation of secrecy commit a tort simply by telling them to [the adoptee].”
In Doe v. Sundquist, the Supreme Court of Tennessee also held that a state law that provided access to original birth records by adoptees over the age of twenty-one did not impede traditional family privacy rights. As was the case with the Oregon law, the Tennessee law included a number of amendments over the years, providing varying degrees of confidentiality protection of birth and adoption records. The court found that the statute providing access just provided “new methods and standards for disclosure,” which “are procedural in nature and reflect the legislature's effort to create legislation that advances the best interest of adopted persons and the public.” The court pointed out that there were limits to disclosure under the statute: disclosure is limited to an adopted individual or that individual's legal representative, [twenty-one] years of age or older. Moreover, extensive provisions are included to allow a birth parent or other related individual to register a “contact veto” and eliminate or reduce the risk that disclosure of identifying information will have a disruptive effect upon the lives of the biological and adoptive families.

The court reiterated the principle that “the confidentiality of records is a statutory matter left to the legislature.” The court also stated that “[a]bsent a fundamental right or other compelling reason, we reject the invitation to extend constitutional protection to the non-disclosure of personal information.”

The United States Court of Appeals for the Sixth Circuit held that Tennessee's retroactive unsealing of adoption and birth records under that law does not violate the constitutional privacy rights of birth parents, adoptive families, or adoption agencies. The court pointed out that the Supreme Court of the United States has not fleshed out the privacy interest in avoiding disclosure of personal matters. The court found that if there is a federal constitutional right to familial privacy, it is not violated by Tennessee's records law.

III. Uses of Social Media in Post-Adoption Search and Reunion

A. Finding Birth Family Through Social Media

This Article is not intended to be a how-to guide on searching social media. Rather, it discusses the uses of social media in general to highlight some of the issues that arise when adoptive children and parents use social media to find their biological relatives. When the person searching knows the current name of the person to be found, some of the first places to look are social media sites, including Facebook, LinkedIn, Twitter, Google+, Myspace, Classmates.com, MyLife, YouTube, Pinterest, and others. These sites are open to the public, generally at no cost. Hundreds of millions of people are connected through internet social media. As of February 2012, Facebook had 845 million active monthly users. Of those, nearly 175 million users were in North America, more than 223 million were in Europe, more than 141 million were in Latin America, nearly 38 million were in Africa, and nearly 184 million were in Asia. Twitter is available in more than twenty languages, and as of September 2011, it had 100 million active users, more than half of whom log in to Twitter daily. As of December 2012, there were more than 637 million registered Twitter users. As of December 2012, Classmates.com had over 40 million users, more than 88% of whom were in the United States. As of April 2012, 170 million users “upgraded” to Google+.

Some adoption reunion registries have utilized social media to expand the accessibility of their services. Some individuals have even created groups in an effort to connect searchers. There is now a private social media site, hosted by the International Soundex Reunion Registry (ISRRxchange), specifically designed for persons “who have been separated from each other by adoption, divorce, foster care, institutional care, abandonment, crisis, etc.” ISRRxchange is a password-protected site which can work in many ways like an interactive mutual consent registry. Members can post their “in search of” (ISO) information on the site and hope for a response. There are also blogs, forums, and other information provided through the
site, as well as friend interactions which look and work much like Facebook. Because the ISRRxchange was not launched until 2012, it is not as well known as some of the other social media sites. Nonetheless, the ISRRxchange holds great promise for those individuals conducting adoption-related searches and should be a regularly-utilized source by searchers. Most of these social media sites are available internationally, so they can reunite family members even in the case of international adoptions. However, for international adoptions, it is also important to maintain a presence on any social media sites which are popular in the foreign country.

As this Article discusses in more detail later, social media sites have various privacy settings which can be configured by the user. People in search will get the most information from profiles with very open privacy settings. People who do not want to be found will either maintain no profile or will restrict the information available to people who have not been accepted as a “friend.” Some sites, such as Google+, allow users to have different levels (or circles, in Google+ parlance) of visible information. Google+ allows users to share posts and pictures selectively to some or all circles.

One problem for many searchers, especially adoptees, is that even if they know the birth mother's name, the mother may have married and assumed her husband's surname. She may have even divorced and remarried, assuming yet another surname. One tip from Pamela Slaton, an investigative genealogist who specializes in adoption searches, is for searchers to try finding their female birth family by searching male family members' pages. Classmates.com is an especially useful site for finding a current surname for a woman whose surname during high school or college is known. Once one family member is found, searching that person's friends, contacts, or connections on social networking sites will often reveal other family members, including female family members with their married surnames. Many social media sites allow users to identify relationships (cousin, aunt, grandmother, sister, etc.), which makes it easier for a searcher to build a family tree of relatives.

Privacy settings on some social media sites allow an otherwise non-“friend” to view portions of that person's profile (such as pictures) by clicking through the profile of another person. Information on social media sites can include names, birth dates, schools attended, hometown, current address, job history, activities, organizations, photographs, blog posts, personal website URLs, Twitter handles, YouTube channels, and other information, which can help confirm the identity of the person being searched for. Pinterest allows people to “follow” particular users or particular boards. If a person is followed, that person's pins will be shown in real time, and any new boards they create will automatically be followed. Every piece of information from one source may provide another link to additional information and social media profiles not yet discovered. Sleuthing through social media has enabled many searchers to find whom they were looking for.

Most adoptees' names are changed as part of the adoption order, usually both the first name and surname. Some birth parents use fictitious names in birth and adoption consent records. As previously mentioned, a birth mother may have married and adopted her husband's surname. Marriages and divorces may have resulted in changed surnames for any female parties concerned. Some people change their names legally for other reasons. Adoptees, birth parents, and siblings may have only the names used at the time of birth and adoption. For people who want to be found, it is important to create a social media presence using the original information. For this reason, Pamela Slaton recommends creating a birth name page. This page allows someone searching for a particular name, birth date, hospital, adoption agency, or other birth- and adoption-specific information to find the profile. Privacy settings should be “public.” Not all identifying information should be posted on this site, however, because imposters may claim to be the searched-for person and seek to financially exploit the person wishing to be found. Further, there are people using adoption search registries and social media sites that include personal and contact information of adoptees and birth parents to extract additional identifying information which can be used in identity
theft. Therefore, the searcher’s current information should be limited to an e-mail address dedicated only to communications relating to the search.

Birth parents also search for their children who have been adopted, sometimes even while those children are minors. Where there is some degree of openness in adoption, social media may be used to facilitate the permitted contact.

*190 B. Learning About Family Members

Once family members have been identified or located, a searcher can use social media to obtain additional information about those family members. Depending on privacy settings, there may be a great deal of information available about those people just from reading information and following links on the person's page. Facebook allows people to subscribe to public postings on a user's timeline without accepting that user as a friend. Some searchers are content having this publicly available information and the ability to view pictures and follow the family member's updates without ever attempting to make contact. They can follow their family members on Twitter and Pinterest and subscribe to their blogs, YouTube channels, and podcasts as interested observers. Other searchers seek to connect with the family member (sending an invitation to be a friend or connection), either to confirm the relationship or to establish ongoing contact. Through one person's site, the searcher may have access to some or all of the people in that person's extended network of friends or contacts, thereby identifying other birth family members. Because many social media profiles specifically identify family relationships among “friends,” the searcher can easily identify additional family members and navigate to those collateral family members' pages to either make contact or to obtain or monitor information about those persons.

If some family members accept a searcher's invitation to connect, it may encourage other family members to also accept an “invitation.” This can build family connections quickly. Depending on the privacy settings of the people involved, being a “friend of a friend” may allow the searcher to view otherwise protected content on the pages of family members who have not been “invited” or who have not accepted the searcher’s invitation. Blogs by friends or connections may include additional information about family members.

*191 C. Staying in Touch

Once the searcher has made contact and is “in reunion,” social media can be a very efficient and economical way to stay in touch. Even if an unconnected family member has not been invited or has rejected an invitation, their posts on a connected family member's page may be visible to the searcher. Similarly, the unconnected person may be able to view posts by the searcher in reunion on the page of the newly-connected family member.

Adoptees and their birth relatives usually cherish current and historical photographs of each other and of other family members. They can post albums of such photographs on their social media pages. Some social media incorporate family tree applications, making it even easier for adoptees to build a family tree for their birth family. Other social media applications allow users to schedule meetings or events and send out invitations, making it easy to plan in-person family reunions. An increasingly popular site is Pinterest, an online virtual pinboard, which allows users to upload photographs, “pin” things found on other sites, organize those images onto topical “boards,” and comment on pinned items. People can browse collections posted by other users and pin the images they find to their own collections. This makes the site useful in search and reunion both in terms of creating a collection, which will be of interest to members within the family and by allowing a user to browse through the interests of family members to learn more about them.
IV. Privacy and Social Media

A. Privacy Settings in Social Media

Members of social networking sites can customize their privacy settings to control what information is available to other users. Many people who fail to adjust their default settings do not realize that these settings allow any member of the public to view all of the information on their social media account. Social media sites such as Facebook are notorious for frequently changing default privacy settings. As of December 2012, Facebook's Data Use Policy includes the following statement:

To make it easier for your friends to find you, we allow anyone with your contact information (such as email address or telephone number) to find you through the Facebook search bar at the top of most pages, as well as other tools we provide, such as contact importers - even if you have not shared your contact information with them on Facebook.

The Data Use Policy provides some examples of information that may be seen even if the user did not make that information public:

*193 If you tag someone, that person and their friends can see your story no matter what audience you selected. The same is true when you approve a tag someone else adds to your story.

Always think before you post. Just like anything else you post on the web or send in an email, information you share on Facebook can be copied or re-shared by anyone who can see it.

Although you choose with whom you share, there may be ways for others to determine information about you. For example, if you hide your birthday so no one can see it on your timeline, but friends post “happy birthday!” on your timeline, people may determine your birthday.

When you comment on or “like” someone else's story, or write on their timeline, that person gets to select the audience. For example, if a friend posts a Public story and you comment on it, your comment will be Public. Often, you can see the audience someone selected for their story before you post a comment; however, the person who posted the story may later change their audience.

Sometimes you will not see a sharing icon when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of stories are always public stories. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.

Facebook now has a new profile called “timeline,” which presents various kinds of information, including a “cover,” “stories,” and “applications.” There are privacy rules which relate to the timeline, including the following discussion in the Data Use Policy:

*194 When you select an audience for your friend list, you are only controlling who can see the entire list of your friends on your timeline. We call this a timeline visibility control. This is because your friend list is always available to the games, applications and websites you use, and your friendships may be visible elsewhere (such as on your friends' timelines or in searches). For example, if you select “Only Me” as the audience for your friend list, but your friend sets her friend list to “Public,” anyone will be able to see your connection on your friend's timeline.
Similarly, if you choose to hide your gender, it only hides it on your timeline. This is because we, just like the applications you and your friends use, need to use your gender to refer to you properly on the site.

When someone tags you in a story (such as a photo, status update or check-in), you can choose whether you want that story to appear on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can remove it from your timeline. Learn more about tagging.

People on Facebook may be able to see mutual friends, even if they cannot see your entire list of friends.

Some things (like your name, profile pictures and cover photos) do not have sharing icons because they are always publicly available. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available. 112

Twitter allows members to send “Tweets,” which are messages of 140 characters or less. 113 Twitter’s privacy policy also starts with a default position that all information tweeted is public:

Our Services are primarily designed to help you share information with the world. Most of the information you provide us is information you are asking us to make *195 public. This includes not only the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet, and many other bits of information that result from your use of the Services. Our default is almost always to make the information you provide public for as long as you do not delete it from Twitter, but we generally give you settings to make the information more private if you want. Your public information is broadly and instantly disseminated. For instance, your public user profile information and public Tweets may be searchable by search engines and are immediately delivered via SMS and our APIs to a wide range of users and services, with one example being the United States Library of Congress, which archives Tweets for historical purposes. When you share information or content like photos, videos, and links via the Services, you should think carefully about what you are making public. 114

Classmates.com is a membership social networking site, with its basic membership available at no cost. 115 According to its privacy policy, the site has a “double-blind” e-mail system for member-to-member communications within the site’s services, making those communications private. 116 However, other communications may be public:

Information and content submitted to comment fields, message boards, events and other public forums on the Services are displayed publicly, so please exercise care in deciding what information and content you wish to disclose. Because this information is publicly displayed through the Services, it may be included in the Services search tools and on third party websites and devices as described in Section 2(i) below. Please keep in mind that, because of the interactive nature of these forums, in many *196 cases you will not be able to remove or revise the information or content that you submit in these areas of the Services and such information or content may remain on the Services even if your membership is terminated. To protect the privacy of our members, we do not allow the public posting of personal contact information . . . .

. . . .

We have created tools to enable you to build a personal profile to share as much information about yourself as you wish. Except as otherwise noted, when you use a specific profile tool all information that you add to your profile is publicly viewable and may be included in the Services search tools and on third party websites and devices as described in Section 2(i) below . . . .
When you find other members, you can view their personal profiles to find out more about them. Every time that you visit another member's profile, your name and the date of your visit will be viewable by that member as someone who visited that member's profile unless you opt out of having your name automatically left on other members' profiles, which you can do by accessing the “Account” section on the Website and changing your preferences. If you opt out of automatically having your name left on other members' profiles, you will still have the ability to leave your name on specific members' profiles on an individual basis.

B. Social Media and Children

There are special rules for the privacy of children using social media sites. The Children's Online Privacy Protection Act of 1998 (COPPA) requires certain protections for children under the age of thirteen using any commercial website which “collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained.” With certain limited exceptions, regulations promulgated under COPPA must:

(A) require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child-

(i) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and

(ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;

(B) require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent, to such parent-

(i) a description of the specific types of personal information collected from the child by that operator;

(ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and

(iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child.

Social media sites have differing policies regarding the participation of minors, and many bar anyone under the age of thirteen from using their sites, regardless of parental consent. For example, Twitter does not knowingly allow minors under the age of thirteen to have an account. Similarly, Google+ does not allow children in the United States who are under the age of thirteen to have accounts, and imposes even higher age requirements for children in Spain, South Korea, and the Netherlands. As of June 2012, Facebook did not allow minors under the age of thirteen to have accounts, but the company is considering having special parent-controlled accounts for those minors. Classmates.com does not knowingly allow any minors to become members. However, users of the sites may well post information about their underage friends and family members, which is then available to people who have access to the users' posts.
Despite these restrictions on children obtaining their own social media accounts, whether on their own or with verified parental consent, many underage children still acquire and use such accounts in violation of the terms of service of the social media sites. This can affect post-adoption searches involving birth parents trying to find their children, underage adoptees trying to find their birth families, and extended family members of both birth parents and adoptees trying to find children in their families.

*200 C. Posting Identifying Information

Posting significant amounts of identifying information is very common on social media sites. However, the user is able to control, to some extent, which identifying information is available to whom. People who want to be found will post enough identifying information to be recognizable to a searcher. The person posting the information may not realize the extent to which other people, who are not specifically authorized by the poster, have access to that information.

Even if a person does not post textual information about his location, this information may be inferred from postings about schools, employers, organizations, groups, and commercial establishments that have been “liked.” A searcher may determine a user's location from information the user does not realize is embedded in a post. Pictures and videos may include geotags, metadata which adds geographical metadata obtained from smart phones and some digital camera connections. This can include identifying where users were when they posted the information online or where a photograph was taken. There are a number of applications for smart phones, tablets, and some cameras which allow geotagged information to be posted on various websites.

Some applications are intended to broadcast the location from which the person is posting. For example, Foursquare allows members to “check in” from various named locations and post the locations on social media sites. People who check in to some commercial sites may be able to get discounts or other benefits while promoting the business they checked into. Such applications allow connections to know where the user is and where the user has been. When a member logs onto Foursquare from a computer, the website asks whether it may track the user's current physical location. Because of the variety of ways in which the user and the user's friends can configure their privacy settings, a location posted from Foursquare may be visible to unintended people.

While Foursquare users intend for their location to be posted online, many are unaware that their location's longitude and latitude coordinates may be included in geotagged metadata, which is then incorporated in any photographs and videos posted on social media websites, such as Facebook, YouTube, and Flickr. While most cameras do not store the photographs' geotagged metadata, most smart phones' default settings use the built-in GPS technology to store this information. Someone accessing the photograph online will be able to determine where the photograph was taken, and possibly even the person's location in real time.

Adoptees and birth parents in search may be able to exploit geotagging to locate where their family members live, go to school, vacation, or frequent. In fact, predators and criminals exploit geotagging for improper purposes, and there are some public awareness efforts to warn people about their inadvertent disclosure of location information.

*202 V. Ramifications of Using Social Media in Post-Adoption Search and Reunion

A. Emotional Issues
In the past, post-adoption searching involved going to the library to search through reference materials and sending out letters requesting records and information.148 There was a time gap before receiving the sought after information, 149 which often caused frustration, but it gave the searcher time for reflection. The Internet has eliminated or at least greatly compressed that time for reflection. For little or no money, anyone with a computer or smart phone can obtain an alarming amount of personal information about almost anybody.150 E-mail communications are sent with a click, unable to be retrieved even if the sender regrets a rash communication.151 Social media allows an aura of intimacy which can mimic what ordinarily takes months or years to establish in a non-Internet based relationship. All of this means that both the searcher and the found person may be dealing with highly charged emotional issues in a highly compressed timeframe.152

For the searcher eager to find long-withheld information and connect with people who are related by blood but not by shared experiences built over time, the reality might be quite different than the expectation.153 The found person is, in most ways, a complete stranger.154 The person may or *203 may not welcome the discovery.155 A birth parent may have wished to keep the fact of the adoptee's existence a secret and may not welcome the contact.156 An adoptee may view the sudden appearance of a birth parent as an intrusion.157 Half-siblings may feel loyalty conflicts in accepting contact without the birth parent's knowledge or approval.158 An adoptee or birth parent may have a highly idealized view of what the searched person will be like and may be bitterly disappointed by the actual person they find.159 A good rule of thumb for searchers is to not embark on the search, or at least not to attempt to make contact, unless they are emotionally prepared for a bad outcome. Once the searcher has identified and located the person searched for, it is wise to be a silent observer for a while before making actual contact through social media.

B. Unwanted Contact and Rejection

1. The Right to Know Is Not the Right to a Relationship

While the searcher has had time to prepare for the contact, the found relative generally has not.160 Even if a birth parent or adoptee has thought about the possibility that the other might be searching, actually being found usually comes as a surprise, at least in terms of the timing.161 Accordingly, the found person generally has not had as much time to prepare for the contact with this close biological relative, a stranger, who may expect immediate acceptance, love, and an ongoing relationship.162 Sometimes that happens, but sometimes it does not.163

*204 People are entitled to associate with whomever they desire. A biological relationship does not guarantee a friendship or ongoing relationship of any kind. When it happens, it can be wonderful. It can also be a nightmare, even for searchers, who may find people with whom they do not really want to maintain a relationship.164 People are, after all, still people, and do not always want to stay in contact with all relatives. Given the compressed timeframe, the expectations built up over years of yearning, and the intensity of the emotions involved, it should not be surprising that some connections are met with rejection, anger, and even hostility.

2. Cyberstalking and Cyberharassment

“Cyberstalking” and “cyberharassment” are terms which informally refer to the unwanted use of the Internet to harass or stalk someone.165 The terms also informally describe a subset of the criminal offenses166 of stalking and harassment using electronic media and formally describe the criminal offense of cyberstalking.167 Stalking and harassment statutes include electronic communications as a method of committing the criminal offense.168 Triggering these offenses generally requires more than accessing someone's social media site that is otherwise available for public access, such as threatening, intimidating,
or using cyberstalking in preparation for another crime. Merely “lurking” on someone's social media profile and monitoring the postings, without more, is unlikely to rise to the level of a crime. Repeatedly making contact with the birth parent or adopted child, threatening to reveal the relationship to others, or threatening to make physical contact is generally construed as the kind of harassment which criminal statutes proscribe. Therefore, although a search may lead to rejection and disappointment, a searcher must not do through social media what would not be permitted in person.

C. Impact on Other Members of the Birth and Adoptive Families

In many cases, a birth parent's other family members are not aware of the adoptee's existence. The birth parent may not want her hand forced in having to reveal the existence of an adopted child to those family members. Some birth parents want to make the disclosure in their own time, while others never want the information to be revealed. Some spouses and children of birth parents feel angry or betrayed by the birth parent. They may feel that the adoptee is trying to intrude upon their family. While some adoptees are embraced by a large and loving birth family, others are seen as a threat, and the family circles the wagons to protect from this intruder. Searchers must be sensitive to the fact that in searching for a birth relative, others may necessarily be impacted, especially when information is posted on that person's social media site, where it may be visible to a wide range of family, friends, business associates, and even casual acquaintances.

Adoption STAR, a nonprofit child placing agency, has promulgated helpful social media recommendations for parties involved in some degree of an open search. These recommendations are equally valid in the context of post-adoption searches:

1. Connecting socially on networking sites exposes each party to the daily happenings of the other person's life. This may be positive, overwhelming or difficult to learn so much about another person. You may learn things you didn't intend or even want to know so evaluate whether it will be healthy to accept a friend request or send a friend request to one another. If you are uncomfortable, then do not be concerned about sending the wrong message. Setting boundaries from the beginning will help you to form a stronger and healthier long-term relationship. You are not saying you do not want to stay connected, but rather you are saying you do want to be connected, just not in this manner.

2. Communication via social networking is forever, so consider what you post before you post something especially if it relates to the adoption process, the adoptive/birth family, or your child.

In conclusion, connecting and maintaining adoption contact via social media sites is new and exciting but can also be overwhelming and challenging. It is “intense” to have this direct and immediate type of contact and if this is the route both birth and adoptive families choose to go, it is important to know you have support available to you through your adoption agency.

It is also imperative to remember two key points: Do all parties feel comfortable with staying connected by way of social media? Have all parties discussed this between themselves before the connection occurs?

VI. Is There Tort Liability for an Unwelcome Search?

The found person can be very upset at being found, at having had personally identifying information concerning the birth and adoption posted on social media sites, or at having the searcher persist in making contact through social media. Searching may involve conduct that can be seen as tortious. This part discusses some possible tort theories and how they may apply to the use of social media in post-adoption searches. The author is not aware of any such actions that were successfully maintained, but is aware that attorneys have sent “cease and desist” letters to some searchers. This section concludes that tort liability should not attach to typical searches through social media.
Consider the following hypothetical search:

Suppose that a thirty-year-old adoptee, Diogenes, has been told that his birth mother was a seventeen-year-old girl who was a senior in high school in New York. The adoptee's amended birth certificate indicates that he was born at a particular hospital in New York City. Using the number on his amended birth certificate, he crosschecks the birth index at the New York Public Library and finds that “Kruptos” was the original surname listed under that birth certificate number. With this information, he presumes that his mother's surname at age seventeen was Kruptos. Because she was a high school senior in January of 1982, the year he was born, she would have been in the high school graduating class of 1982. Because she was seventeen when he was born, she would have been born around 1965. He had been given non-identifying information indicating that his mother had brown eyes and black hair and that she enjoyed sports. His adoptive family was told the birth mother had been referred to as Cassie. Armed with this information, Diogenes posts the following information on various social media registries and search groups:

Adoptee ISO birth mother, maiden name Cassie Kruptos, approximate d.o.b. 1965. She went to high school in New York, class of 1982. Brown eyes, black hair, involved in sports. My d.o.b. is 1/1/82. Anyone with any information, please contact Diogenes.

Various people respond to his posts, and he is directed to the profile of Cassandra Anakribis, a forty-seven-year-old woman living in a rural area of upstate New York.* This information seems to be a match, so he searches various social media sites for Cassandra Anakribis and finds her profile on Facebook. Her timeline includes many pictures of her, her husband, her children, and her new grandchild. From reading the information she has posted, he can see that she was involved in sports at her New York City high school and that she has brown eyes and black hair. Her birthday is October 31, 1964, which would have made her seventeen when Diogenes was born. Among her seventy-five friends are several people with the surname Kruptos, who are identified as “family.” He is now convinced that Cassandra Anakribis is Cassie Kruptos, his birth mother. His “friend” invitation to Cassandra is accepted. He sends her a private message through Facebook saying that he is her son, whom she surrendered for adoption in 1982, that he is doing well, and that he wants to make contact. After getting no response, on October 31 he posts on her timeline: “Happy birthday, Mom. I am so glad I found you after all these years!” In response to that post, one of Cassandra's children sends him a private message: “Who are you, and why are you calling my mother Mom?” He responds by private message: “When our mother was seventeen, she had a child out of wedlock—me. I was adopted into a wonderful home and have had a great life. I have always wondered about my birth mother, and I am thrilled to have found her and all of you, my brothers and sisters and now a new nephew. I only live a few hours away and would love to come visit and meet you all.”

A. Defamation

The Restatement (Second) of Torts sets out the elements of a cause of action for defamation as follows:

To create liability for defamation there must be:

(a) a false and defamatory statement concerning another;

(b) an unprivileged publication to a third party;

(c) fault amounting at least to negligence on the part of the publisher; and

(d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication.*

The Restatement says that “[a] communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.” Does a communication
implying or stating that a woman had a child who was adopted by a third party harm the reputation of the woman? As applied to other possible search scenarios, the questions would be: Does the fact that a man fathered a child who was adopted by a third party harm the reputation of the man? Does the fact that a person was adopted harm the reputation of that person? Fifty or one hundred years ago, the answer would probably have been yes. But would a reasonable person in the twenty-first century consider such a communication to harm the birth mother's reputation? Probably not. Nevertheless, assuming for the sake of argument that such a communication would be considered defamatory, the communication still might not be actionable.

“Publication” of defamatory statements is a term of art which simply relates to “communication intentionally or by a negligent act to one other than the person defamed.” Accordingly, making what might be considered a defamatory accusation to someone directly cannot be a publication unless the communication is also received by a third party, such as a post on a social media site rather than a private message to the person about whom the statement is made. The First Amendment's freedom of speech is a broad right. However, its protection of false, defamatory speech is narrower when the speech involves statements concerning private persons as opposed to public figures. The Restatement (Second) of Torts describes the tort of defamation as applied to a private person as follows:

One who publishes a false and defamatory communication concerning a private person . . . is subject to liability, if, but only if, he

(a) knows that the statement is false and that it defames the other,

(b) acts in reckless disregard of these matters, or

(c) acts negligently in failing to ascertain them.

Presumably, the searcher will not knowingly post false information, because the searcher wants to find the family member. However, in the initial stages of a search, a very broad net might be cast to find the correct person. Consider again the hypothetical about Diogenes: Diogenes posted somewhat identifying information about Cassie Kruptos, whom he identified as his birth mother, on social media sites devoted to adoption searches. In reading the post, a reasonable person would conclude that Cassie Kruptos from New York, who graduated high school in 1982, gave birth to and placed a child for adoption. People who knew Cassie in high school would know that she was not married at the time and could infer that she had given birth to a baby out of wedlock. Further, in posting his birthday greeting to Cassandra, Diogenes identifies her as his mother. People who know her may not believe she has a son named Diogenes. Further, he specifically told Cassandra's son that he was Cassandra's child, born out of wedlock. These Facebook communications, visible to people other than Cassandra herself, are increasingly more specific-arguably defamatory-representations.

Since truth is an absolute defense to defamation, if Diogenes has found the right person, Cassandra cannot successfully maintain a defamation action against him. Nevertheless, suppose that his information is incorrect. Suppose that it was Cassie's classmate who had become pregnant, and to hide her own identity, she falsely used Cassie's name and other identifying information at the hospital when filling out the birth certificate and in dealing with the adoption agency. In that event, Diogenes may have found the right Cassie Kruptos, but she was not, in fact, his birth mother. In that case, truth would not be an absolute defense. The inquiry would then turn on whether he acted in reckless disregard of the truth or negligently in failing to ascertain the truth.

The private message Diogenes first sent to Cassandra would not be actionable because it was not communicated to a third party. However, the post on her Facebook profile and the private message to her son were communications to third parties, which could possibly trigger liability if the statements were considered defamatory. Although the communications are not likely to be considered defamatory, even if they were, there are conditional privileges related to defamation even when the communications are false. The conditional privileges require showing that the publisher had knowledge or reckless
disregard as to the falsity of the communication—mere negligence is not enough to sustain liability. \footnote{197} \footnote{213} Section 594 of the Restatement (Second) of Torts provides a conditional privilege for the protection of the publisher's interest: An occasion makes a publication conditionally privileged if the circumstances induce a correct or reasonable belief that

(a) there is information that affects a sufficiently important interest of the publisher, and

(b) the recipient's knowledge of the defamatory matter will be of service in the lawful protection of the interest. \footnote{198}

The comment to subsection (a) notes the publisher's interest must be one that is not entirely outside the range of direct or indirect legal protection \footnote{199} The following example is given: [T]he interest may be one which, while not sufficiently important to receive direct legal protection, is sufficiently important to receive indirect protection by a privilege to defend it by reasonable invasions of the interests of others, such as their interest in reputation. Thus the interest of a parent in the social and moral welfare of his child, while insufficient to support an action by the parent against another whose conduct has been detrimental to the child's well-being, is sufficient to support a conditional privilege on the part of the parent to publish defamatory matter concerning another for the purpose of protecting or advancing the child's well-being. \footnote{200}

What happens when the "child," whose well-being is at issue, is now the adult adoptee and the other person is the adoptee's birth parent? In this instance, the publisher certainly has an important interest in his own genetic connectedness. The Restatement (Second) makes special reference to family matters by providing a discreet conditional privilege for family relationships: \footnote{214}

(1) An occasion makes a publication conditionally privileged if the circumstances induce a correct or reasonable belief that

(a) there is information that affects the well-being of a member of the immediate family of the publisher, and

(b) the recipient's knowledge of the defamatory matter will be of service in the lawful protection of the well-being of the member of the family.

(2) An occasion makes a publication conditionally privileged when the circumstances induce a correct or reasonable belief that

(a) there is information that affects the well-being of a member of the immediate family of the recipient or of a third person, and

(b) the recipient's knowledge of the defamatory matter will be of service in the lawful protection of the well-being of the member of the family, and

(c) the recipient has requested the publication of the defamatory matter or is a person to whom its publication is otherwise within generally accepted standards of decent conduct. \footnote{201}

Application of this privilege goes to the heart of who is "family." While the law of adoption may legally extinguish the parent-child relationship between the adoptee and his birth mother, \footnote{202} the quintessential truth of the matter is that she always will be his birth mother, and no human law can change that biological fact.

There is a related conditional privilege for protecting the interest of the person receiving the information and for protecting the interest of a third person. \footnote{203} Section 595 of the Restatement (Second) provides:

(1) An occasion makes a publication conditionally privileged if the circumstances induce a correct or reasonable belief that
(a) there is information that affects a sufficiently important interest of the recipient or a third person, and

(b) the recipient is one to whom the publisher is under a legal duty to publish the defamatory matter or is a person to whom its publication is otherwise within the generally accepted standards of decent conduct.

(2) In determining whether a publication is within generally accepted standards of decent conduct it is an important factor that

(a) the publication is made in response to a request rather than volunteered by the publisher or

(b) a family or other relationship exists between the parties. 204

With respect to communications between adoptees and their birth families, the adoptee can truthfully say that “a family or other relationship exists between the parties.” 205 Does a birth parent have an important interest in being found? Is it indecent for a son or daughter to contact his or her own birth mother or other biological relatives? Many birth mothers experience ongoing pain and shame concerning the surrender of the child for adoption, and being found can heal wounds and positively impact their well-being. While it is true that being found might also have the opposite effect, 207 an adoptee may certainly have a “reasonable belief” that the results of the search would be of service in the lawful protection of the mother's well-being.

The Restatement (Second) of Torts further provides that “[a]n occasion makes a publication conditionally privileged if the circumstances lead any one of several persons having a common interest in a particular subject matter correctly or reasonably to believe that there is information that another sharing the common interest is entitled to know.” 208 The “right to *216 know” has long been a hallmark of the adoptee rights movement: a person has the inherent right to one's own identity and history, including the knowledge of one's genetic roots. 209 Diogenes could certainly argue that his mother and brother have a common family interest and are “entitled to know” that they are related, regardless of whether they choose to act on that knowledge and develop an ongoing social relationship.

Even if Diogenes' communication is factually false and defamatory, and even if he is entitled to a conditional privilege, he is nevertheless “subject to liability . . . if he abuses the privilege.” 210 The privilege is “conditioned upon the manner in which the privilege is exercised.” 211 The privilege may be lost if the publication is not made “for the purpose of protecting the interest for the protection of which the privilege is given.” 212 The Restatement (Second) of Torts explains in a comment: [A] publication of defamatory matter upon an occasion giving rise to a privilege, if made solely from spite or ill will, is an abuse and not a use of the privilege. However, if the publication is made for the purpose of protecting the interest in question, the fact that the publication is inspired in part by resentment or indignation at the supposed misconduct of the person defamed does not constitute an abuse of the privilege. On the other hand, if the publisher does not act to protect the interest in question, the privilege is abused although he is not acting from spite or ill will. 213

The conditional privilege may also be abused if, in addition to publishing the privileged matter, “he also publishes unprivileged defamatory matter.” 214 The comment to section 605A of the Restatement summarizes other sections, which address how this abuse may occur:

It applies, for example, when the defendant, upon such an occasion, communicates a statement that he believes to be *217 true and adds a statement that he knows to be false. (See § 600). It applies when one statement is communicated for the purpose for which the privilege is given and the other is added for a purpose that is foreign to the privilege. (See § 603). It applies also when the one statement is reasonably
believed to be necessary in order to accomplish the purpose of the privilege and the other is not. (See § 605). 215

So long as Diogenes does not abuse the privilege, Cassandra should not succeed in bringing a defamation action based on his communications to her or to her son, even if she is not his birth mother.

B. Publicity Given to Private Life

The right of privacy was first articulated in an 1890 law review article by Samuel D. Warren and Louis D. Brandeis. 216 At the time the article was written, and up until 1925, the First Amendment had not yet been applied to the states through the Fourteenth Amendment. 217 However, the privacy torts described by Warren and Brandeis were incorporated into the Restatement (Second) of Torts via the reformulations of Dean Prosser. 218 Unlike defamation, the tort of publicity given to private life does not involve false statements. 219 This cause of action in tort is derived from the *218 right of privacy. 220 The Restatement sets out the elements of a cause of action as follows:

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

(a) would be highly offensive to a reasonable person, and

(b) is not of legitimate concern to the public. 221

“Giving publicity,” as used in this explanation, does not have the same meaning as “publishing” in context of the tort of defamation. 222 The comment to the Restatement explains:

“Publicity” . . . means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge. The difference is not one of the means of communication, which may be oral, written or by any other means.

It is one of a communication that reaches, or is sure to reach, the public. 223

This raises the question of who comprises the “public” to which the private information should not be disclosed. There is a difference in degree, if not in kind, between publishing information in a large circulation newspaper (or its online equivalent, such as the Huffington Post) 224 and posting a comment on someone's personal Facebook profile. 225 Can one's *219 self-defined boundaries of social media be said to define who is and is not “the public?” Posting the true fact of one's genetic connection to members of a family may well be considered a matter of legitimate concern to those invited into one's cyber social circle. However, certain privacy settings may allow outsiders access to the posted information, despite intentions to contain the information within the cyber circle. 226 Because privacy settings are clearly disclosed on social media sites, 227 the site's users have, at least, imputed knowledge of those settings. By customizing or accepting the default settings, users may in essence be consenting to exposure of private information to individuals outside the users' circles. Much of what is posted on social media sites today would have been considered highly private information only a generation or two ago. 228 Many social media users have essentially flung open the doors of their lives, and it should come as no surprise that users who give others the ability (hence, the implied permission) to post personal search-related information on the users' pages, cannot assert that those actions violate privacy. 229
Giving birth to a child is a private matter, but the birth is a publicly recorded event. Although birth records may be sealed, the information may be publicly reported prior to the sealing. The birth parent lost parental rights through voluntary surrender or involuntary termination. The adoptive parent became the legal parent upon the subsequent adoption. Therefore, the privacy of the adoption should no longer be a birth parent's concern, but rather a concern of the adoptive parent. Would disclosure of that information be “highly offensive to a reasonable person?” That kind of information might have been offensive fifty or one hundred years ago, but it is unlikely to be deemed “highly offensive” in the twenty-first century. The Restatement (Second) of Torts points out: “The protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens.” The Internet has drastically changed “the customs of the time and place,” and it has eroded social media users’ privacy expectations.

Furthermore, the private information is not only that of the birth parent but also of the adoptee. The disclosures in question directly involve the interests of both the mother and the child. From the adoptee's point of view, it should not be a matter of shame that the child was born or that the child now presents himself or herself to the mother and the genetic maternal family. Can it be offensive for a person to reveal private information about himself or herself just because that information necessarily implicates others who are involved?

The Restatement provides a special note with respect to a cause of action for publicity given to private life:

This Section provides for tort liability involving a judgment for damages for publicity given to true statements of fact. It has not been established with certainty that liability of this nature is consistent with the free-speech and free-press provisions of the First Amendment to the Constitution, as applied to state law through the Fourteenth Amendment.

One possible modification to the public disclosure tort in the context of social networking would be to “adjust[] the First Amendment analysis to ensure that any speech deterred is only the most embarrassing, harmful, and utterly devoid of any social purpose.” Consider the Diogenes hypothetical under this suggested reformulation. Diogenes had a valid social purpose: to make a connection with his birth mother and her extended family. Simply because she may have declined to accept the connection does not render Diogenes' purpose in making the disclosure improper. There should be no tort liability under this cause of action for any of Diogenes' communications.

The Supreme Court of North Carolina addressed this tort in Hall v. Post, which involved an action brought by a woman and her adoptive mother against a reporter and newspaper that printed two articles regarding the birth mother's search. The defendants argued that “the imposition of civil liability for their truthful public disclosure of facts about the plaintiffs would violate the First Amendment . . . .” The court pointed out that “[t]he private facts branch of the invasion of privacy tort was not recognized at common law in 1776 or at the times of adoption of either the Constitution or the Bill of Rights. It has never been recognized in . . . [any of the] jurisdictions” that share “the heritage of the English common law.” The court rejected the viability of the tort as applied to true facts, stating:

[An]y possible benefits which might accrue to plaintiffs are entirely insufficient to justify adoption of the constitutionally suspect private facts invasion of privacy tort which punishes defendants for the typically American act of broadly proclaiming the truth by speech or writing. Accordingly, we reject the notion of a claim for relief for invasion of privacy by public disclosure of true but “private” facts.

Under the Hall analysis, the entire cause of action was eliminated as a matter of constitutional law. This analysis would also provide a defense for Diogenes, whose disclosures were even more limited. Even if the entire cause of action is recognized, as
it is in most jurisdictions, a robust constitutional defense should shield Diogenes from liability because of the limited nature of his disclosures. 247

C. Intrusion upon Seclusion

Another privacy tort is the tort of intrusion upon seclusion, which does not require any communication to a third party but relates strictly to the defendant's contact with the plaintiff. 248 The Restatement (Second) of Torts sets out the elements of this cause of action as follows: “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” 249 The most frequent use of this tort involves a physical intrusion, such as entering the person's physical space *224 or taking a photograph of the person in a nonpublic place. 250 In fact, the Restatement provides: Thus there is no liability for the examination of a public record concerning the plaintiff, or of documents that the plaintiff is required to keep and make available for public inspection. Nor is there liability for observing him or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye. Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters. 251

Social media, by its very nature, is analogous to a “public place.” 252 Perhaps closed chat rooms, instant messages, private messages, or members-only sections of social media sites are not exhibited to the public gaze, but the vast majority of what is on social media sites is, in fact, available to the public. 253 Diogenes did not purloin sealed records to locate Cassandra. He did not hack into her private social media profile. He did not enter into her physical space in any way. He used what was publicly available. Cassandra chose to engage in the cyberworld of social media in a way that allowed Diogenes to enter, which she was free to rebuff. Some *225 social media sites allow users to block certain people from access which otherwise might have been publicly viewable. 254 While Diogenes' contact may have been unwelcome, it was not so intrusive that it should be considered tortious.

It is challenging to apply torts created to address entirely different scenarios to the world of social media. It has been pointed out that “[n]ew technologies have enabled novel social situations that generate privacy harms and concerns that were unforeseeable by the Restatement's authors.” 255 While there have been proposals for new privacy laws dealing with the Internet, 256 these mostly address commercial use or misuse of information, 257 consumer profiling, 258 or governmental aggregation of information. 259

*226 VII. Where Do Adoptees' Rights to Publicize Their Own Family History End and the Birth Families' Rights to Privacy Begin?

The Supreme Court of the United States has pointed out that privacy cases have involved at least two different interests: “One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.” 260 The first interest was described in Justice Brandeis's dissent in Olmstead v. United States 261 as “the right to be let alone.” 262 The second interest involves “matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.” 263 For the adoptee, knowledge of one's biological family is a crucial step in acquiring family medical history, which is an important factor in many health care decisions. 264 When most now-adult adoptees were adopted, there were not as many genetic medical conditions and predispositions known as there are today. 265
Even if a careful medical history of the birth family had been taken prior to the adoption, many birth mothers were young and likely did not yet show signs of conditions with which a family history is associated. The U.S. Department of Health and Human Services has launched a national public health campaign, called the Surgeon General's Family History Initiative, “to encourage all American families to learn more about their family health history.” The Office of Public Health Genomics (OPHG) started the Family History Public Health Initiative “to increase awareness of family history as an important risk factor for common chronic diseases such as cancer, heart disease, and diabetes, and to promote its use in programs aimed at reducing the burden of these diseases in the U.S. population.”

Everyday Health's website proclaims “[k]nowing the past can help create a healthier future.” The site states that “family medical history should include both sides of your family, with your siblings, parents, grandparents, aunts and uncles, and nieces and nephews.” Without knowing one's family medical history, many risk factors cannot be assessed, and the ignorant adoptee cannot make informed decisions about preventive measures or lifestyle changes which are influenced by family risk factors. This ignorance affects not only the adoptee, but the adoptee's children as well.

Aside from the medical aspect, knowing the past can also create a healthier psychological state in the present and future for the adoptee. People who have no ability to acquire knowledge about their genetic heritage may experience “genealogical bewilderment” or loss of “genetic ego.” This goes far beyond “mere curiosity” and involves the breach of the relationship formed in utero and broken at a time when the infant did not have the cognitive or verbal capacity to encode or deal with the separation. The Evan B. Donaldson Adoption Institute has written that “[s]eeking identifying information relating to one's birth is typically a means to an end of gaining information, closure, an authentic sense of one's own identity, and sometimes the opportunity for a relationship with birth family members.”

As a necessary biological fact, a child has parents. Whatever legal changes may be made to the parent-child relationship, the biological relationship remains. The parent and child have a shared biological history. Children are branches on a genetic family tree, which has roots and other branches. While the adoptee may have been legally pruned from that family tree, the medical and social history of the entire family tree remains a part of that child's inherent birthright.

Even outside of the adoption context, people talk about their family members and family interactions, often sharing information that other family members might consider embarrassing or private. Children and parents embarrass each other and tell private stories that the other wishes they had not. Social media postings certainly include information that a reader might presume would be unwelcome by the poster's family members. One of the weaknesses of the immediacy of Internet communication is that people can communicate without adequate time for reflection, resulting in negative ramifications from employers, co-workers, friends, and family.

The adoption context should be no different, at least where tort liability is concerned. To communicate the fact of a genetic relationship online is to say something about oneself, although it may implicate other members of the birth family. Adoptees and birth parents should be considerate of and sensitive toward one another. That is good manners. That is what should be expected in all interpersonal communications among all people. However, the law does not regulate manners.

No person should be denied the right to claim and proclaim their own genetic heritage. There may be no legal rights that flow from biological relationships, such as rights of inheritance or the right to be present at the hospital bedside of a relative. Likewise, there should be no legal liability attached to stating true facts, however inconvenient they may be to other family members. The birth family's legal right to privacy should be no greater than any other family's right to privacy, and certainly, it should not be in derogation of the adoptee's rights to personhood, affiliation, and personal history.
VIII. Conclusion

Social media will remain an important tool for both post-adoption searches and post-search contact. For those searching, social media is a window through which much publicly available information can be found. There is no reason that birth family members should be excluded from using Internet resources to make connections and learn information about one another.

Outside of the adoption arena, many parents and children exchange and monitor information about one another through available Internet resources. Indeed, it is likely that for many parents, their knowledge about their adult children's day-to-day lives may come more from viewing their children's social media postings than from direct conversations. Young people may text, instant message, and e-mail their friends more than they actually interact with one another in person. Social media has become the gathering place for the generations living in the twenty-first century. It can be a safe meeting place for birth families to find and get to know each other and to stay in touch, with or without making in-person contact. The adoptee and birth family share a history, with overlapping pieces of information and a common ancestral background. Each should have the right to explore and communicate that history without being found to have abridged the privacy of the other. Social media has become, and is likely to remain, a significant forum within which to carry on that exploration.

*Appendix: Statutory Access to Birth & Adoption Records*

**Ala. Code § 22-9A-12(c) (LexisNexis 2006)**

Adoptee that is nineteen years old or older may obtain a noncertified copy of the original birth certificate and any evidence of the adoption, legitimation, or paternity determination held with the original record upon written request.

**Alaska Stat. § 18.50.500(a) (2010)**

Adoptee that is eighteen years old or older may obtain an uncertified copy of the original birth certificate and any change in the biological parent's name or address attached to the certificate upon request.

**Alaska Stat. § 18.50.510(a) (2010)**

Adoptee that is eighteen years old or older may obtain specified types of non-identifying descriptive information about the birth parents, if available.


Adult adoptees may obtain a noncertified copy of the unaltered original birth certificate if both birth parents have filed a contact preference form authorizing release.

If only one parent has consented, the nonconsenting parent's information is redacted. An adoptee that is eighteen years old or older may inspect and copy all adoption records relating to adoptions finalized on or after September 1, 1999, and he or she may obtain all adoption records if the birth parent is deceased except for the name of the nonconsenting living birth parent.

**Del. Code Ann. tit. 16, § 3110(b) (2003)**

Adoptee that is twenty-one years or older may obtain a noncertified copy of a vital record, including an original birth certificate upon application.
If it is verified that a birth parent of the adoptee is deceased, the name and place of burial of the deceased biological parent, if known, may be disclosed without a court order.

Adoptees born prior to January 1, 1946, may obtain a noncertified copy of the original birth certificate. An adoptee that is twenty-one years or older and was born on or after January 1, 1946, may obtain a noncertified copy of the original birth certificate, but if the birth parent who is still alive has vetoed disclosure, then information about that parent will be redacted from the copy.

Adoptees whose adoption became final prior to July 4, 1941, and whose adoption record was not required to be sealed at the time, need not prove good cause to unseal adoption record, subject to the court's consideration of a birth parent's affidavit requesting nondisclosure of identity.

Adoptees of legal age may obtain a certified copy of the original birth certificate or abstract attached thereto upon demand.

Adoptee that is eighteen years old or older, adoptee's attorney, or, if the adoptee is deceased, the adoptee's descendants may obtain a noncertified copy of the unaltered original birth certificate.

Adoptee that is twenty-one years old or older may receive a copy of the original birth certificate, all records that relate to the adoptee's new certificate of birth, if any, and the report of the adoptee's order of adoption filed by the clerk of court.

For adoptions in which the former parents' rights were terminated on or after May 28, 1945, and before September 12, 1980, an adult adoptee may obtain identifying information regarding a birth parent who consents or is deceased; for adoptions in which the former parents' rights were terminated before May 28, 1945, or on or after September 12, 1980, an adult adoptee may obtain identifying information except for information relating to a living birth parent who has filed a statement currently in effect with the central adoption registry denying consent to have identifying information released.

Adoptee who was adopted on or before July 1, 1967, may obtain a copy of the original birth certificate upon written request; an adoptee that is eighteen years old or older who was adopted on or after October 1, 1997, may obtain a certificate of adoption that states the date and place of adoption, the date of birth of the adoptee, the name of each adoptive parent, and the name of the adoptee as provided in the decree, as well as a copy of the original birth certificate upon written request unless the birth parent has requested in writing that the original birth certificate not be automatically released.
Adoptee may obtain all information on the original birth certificate if both birth parents are deceased or if one birth parent is known and such parent is deceased and no nonconsent form has been filed by a biological parent.

*Neb. Rev. Stat. § 43-146.06 (2008)*

Failure by a birth parent to sign the notice of nonconsent shall be deemed a notice of consent by such parent to release the adoptee's original birth certificate.

*Neb. Rev. Stat. § 43-146.09*

Adoptee may obtain all information on the adoptee's original birth certificate if both birth parents are deceased or only one birth parent is known and that parent is deceased.

*N.H. Rev. Stat. § 5-C:9(I)-(I-a) (LexisNexis 2008)*

Adoptee that is eighteen years old or older may obtain a noncertified copy of the unaltered, original birth certificate, and if they have been filed by the birth parent, a contact preference form and an updated medical history form.

*Okla. Stat. Ann. tit. 10, § 7505-6.6(D) (West 2009)*

Upon submission of proof of identity and an affidavit in which the adopted person states under oath that such person does not have a biological sibling under the age of eighteen who is currently in an adoptive family and whose location is known to the adopted person, an adult adoptee who was adopted after November 1, 1997, may obtain a copy of the original birth certificate unless the birth parent has filed an unrevoked affidavit of nondisclosure, in which case identifying information about that parent will be redacted.


Adoptee that is twenty-one years old or older may obtain a certified copy of his/her unaltered, original, and unamended birth certificate, and if one has been filed by the birth parent, a contact preference form.

*R.I. Gen. Laws § 23-3-15(g)(1)*

Effective July 2, 2012, an adult adoptee may obtain a noncertified, original birth certificate.

*Tenn. Code Ann. § 36-1-127(b), (c) (2010)*

Adoptee that is twenty-one years old or older may obtain adoption records, sealed records, sealed adoption records, post-adoption records, or other records or papers relating to the adoption or attempted adoption of a person, subject to a birth parent's contact veto.


Adult adoptee who knows the identity of each parent named on the original birth certificate is entitled to a noncertified copy of the original birth certificate without obtaining a court order.
For adoptions finalized on or after July 1, 1986, an adoptee that is eighteen years old or older may obtain identifying information unless the birth parent filed a request for nondisclosure.


Adoptee who has attained the age of eighteen and who has access to identifying information may obtain a copy of the original birth certificate; ninety-nine years after the adoptee's birth, the original birth certificate is unsealed and becomes a public record.


Adoptee that is eighteen years old or older and whose adoption was finalized after October 1, 1993, may obtain a noncertified copy of the original birth certificate unless the birth parent has filed an affidavit of nondisclosure.

Footnotes

a1 Ann M. Haralambie is a Certified Family Law Specialist, Arizona Board of Legal Specialization, in private practice in Tucson, Arizona, an author, and a speaker. She is also an adoptee now in reunion after a thirty-five year search for her birth family.

1 In re Carroll's Estate, 68 A. 1038, 1039 (Pa. 1908).

2 See Elizabeth J. Samuels, The Idea of Adoption: An Inquiry into the History of Adult Adoptee Access to Birth Records, 53 Rutgers L. Rev. 367, 369 (2001). As late as 1960, “some forty percent of the states still had laws on the books recognizing an unrestricted right of adult adoptees to inspect their original birth certificates.” Id. It was “only in the 1960s, 1970s, and 1980s that all but three of those states changed their laws to close birth records to adoptees.” Id. The Colorado Court of Appeals concluded that based on the history and evolution of Colorado adoption laws, from 1951 to 1967, records of adoptions were not available to the public without a court order but were available to the parties involved in the adoption process. See In re J.N.H., 209 P.3d 1221, 1225 (Colo. App. 2009). The court found that the legislature intended for adoptions finalized after 1951 but before July 1, 1967, to be treated differently than those adoptions finalized after July 1, 1967. Id. at 1226. “And this legislative history confirms to us that the concept of ‘anonymity’ of the parties to an adoption necessarily depends upon the sealing of court records to make them accessible only through a specific process.” Id. As a result of that analysis, the court held that “for adoptions finalized prior to July 1, 1967, but after July 1, 1951, an adoptee may have access to the names of his or her birth parents and to all court records and papers regarding the adoption.” Id.

3 See infra Appendix.


6 See, e.g., Alma Soc'y Inc. v. Mellon, 601 F.2d 1225, 1227-29, 1233, 1236, 1238 (2d Cir. 1979); In re Roger B., 418 N.E.2d 751, 754, 756-57 (Ill. 1981); In re Adoption of S.J.D., 641 N.W.2d 794, 803 (Iowa 2002); In re Maples, 563 S.W.2d 760, 762, 764 (Mo. 1978); cf. In re Estate of McQuesten, 578 A.2d 335, 339 (N.H. 1990) (“If all of the parties to the adoption give their consent to unsealing the adoption records . . . the State still has an interest in continued confidentiality. Even in a[n] . . . ‘open’ adoption . . . court records could contain potentially embarrassing information and be disruptive to the relationship between children and their adoptive parents.”).


8 See id. at 22-23.


See id. at 11. The U.S. Department of Health and Human Services Children's Bureau includes tips on the use of social media in postadoption searches in its fact sheet. See id. at 11-12.

Id. at 11.

See id. at 2.

See Eileen Fursland, Facing up to Facebook 2-3, 22, 27-30, 89, 90-92 (2010) (discussing how the Internet, social networking, and other technologies are changing the landscape of adoption contact, search, and reunion).

See, e.g., Does 1, 2, 3, 4, 5, 6, and 7 v. State, 993 P.2d 822, 833-36 (Or. Ct. App. 1999).


Does 1, 2, 3, 4, 5, 6 and 7, 993 P.2d at 825.


Id.


Int'l Soundex Reunion Registry, supra note 9.


See What Is the ISRRxchange?, supra note 56.

Compare Classmates.com Social Networking Website, supra note 51, and Countdown to 500 Million Registered Twitter Accounts, supra note 50, and Fach, supra note 46, and Kaushik, supra note 52, and One Hundred Million Voices, supra note 49, with ISRRxchange, supra note 57 (comparing the number of users on Facebook, Twitter, Classmates.com, Google+, and ISRRxchange).

Paslawsky, supra note 44, at 1487.


See id.


See Family Safety Center, Google, http://www.google.com/goodtoknow/familysafety/sharing/ (last visited Dec. 16, 2012) (“We designed Google+ with privacy in mind. A number of different features provide you with transparency and choice over who can see what type of information you post or share, including circles which allow you to select exactly who sees your posts, notification settings which allow you to specify who can contact you, and visibility settings allowing you to make your profile private.”).
Pamela Slaton is the author of Reunited: An Investigative Genealogist Unlocks Some of Life's Greatest Family Mysteries (2012) and was host of the 2011 television show Searching for . . . on the Oprah Winfrey Network. She also has a website at http://www.Pamelaobr.com.


Fact Sheet 35: Social Networking Privacy: How to be Safe, Secure and Social, supra note 63.


Id.

See, e.g., Fursland, supra note 17, at 38-39 (discussing the ways Facebook allows users to link and interact with others online).


Interview with Pamela Slaton, supra note 68.

Cf. Fursland, supra note 17, at 49-50 (noting that many birth parents may not be able to find their children through a simple name search on social networking sites, but that it can be possible to find an adopted child even without the child's new surname by using other known information).

See id. at 32.

See id. at 36-37; Metro Reunion Registry, supra note 9. Metro Reunion Registry notifies users that only a certain portion of their information will be accessible on the website and warns them of scams that target registries that post personal and contact information. Metro Reunion Registry, supra note 9. The website also provides a link to an actual scam e-mail sent to an adoptee in which the scammer attempted to obtain more information under the guise of transferring money from a Swiss bank account set up by the birth parents. Id.


See Macdonald, supra note 86.


See Macdonald, supra note 86.


Id.

See Choose Who You Share with, supra note 90.


See Child Welfare Info. Gateway, supra note 13, at 11 (noting that it is free to join social media sites like Facebook and that social networking sites offer a way to connect people without the need for travel and other expenses).

See id. at 11-12.

See id.

See id. at 12.

See Cooley, supra note 87 (discussing social media tools, such as blogs, Facebook, and Twitter, that allow users to share pictures).


See Getting Started, supra note 73.

See id.

See Understanding Social Networking Site Privacy Settings, supra note 62.

See Fursland, supra note 17, at 45-46.

See id. at 45.


Id.


Data Use Policy: Sharing and Finding You on Facebook, supra note 109.

About Twitter, supra note 48.

About Us, supra note 70.


Id.

See Fursland, supra note 17, at 47 (providing examples of privacy restrictions on Facebook users who are under eighteen years old); Susan Hanley Duncan, MySpace Is Also Their Space: Ideas for Keeping Children Safe from Sexual Predators on Social-Networking Sites, 96 Ky. L.J. 527, 546-47 (2008).


The regulations are codified at 16 C.F.R. §§ 312.1-312.12 (2012). The Federal Trade Commission adopted final COPPA rule amendments, which take effect on July 1, 2013. The final amendments do the following:

[1] modify the list of “personal information” that cannot be collected without parental notice and consent, clarifying that this category includes geolocation information, photographs, and videos;
[2] offer companies a streamlined, voluntary and transparent approval process for new ways of getting parental consent;
[3] close a loophole that allowed kid-directed apps and websites to permit third parties to collect personal information from children through plug-ins without parental notice and consent;
[4] extend coverage in some of those cases so that the third parties doing the additional collection also have to comply with COPPA;
[5] extend the COPPA Rule to cover persistent identifiers that can recognize users over time and across different websites or online services, such as IP addresses and mobile device IDs;
[6] strengthen data security protections by requiring that covered website operators and online service providers take reasonable steps to release children’s personal information only to companies that are capable of keeping it secure and confidential;
[7] require that covered website operators adopt reasonable procedures for data retention and deletion; and
[8] strengthen the FTC's oversight of self-regulatory safe harbor programs.


Twitter Privacy Policy, supra note 114 (“Our Services are not directed to persons under 13. If you become aware that your child has provided us with personal information without your consent, please contact us at privacy @twitter.com. We do not knowingly collect personal information from children under 13. If we become aware that a child under 13 has provided us with personal information, we take steps to remove such information and terminate the child's account.”).


Privacy Policy, supra note 116 (“Minors (those under 18) are not eligible to use the Services, and we ask that minors not submit any personal information to us or use the Services. We will not knowingly allow minors to become members. If we later learn that a minor is a member, then that minor’s membership will be terminated.”).


See Julie Brill, Privacy & Consumer Protection in Social Media, 90 N.C. L. Rev. 1295, 1301 (2012) (“[I]n May of this year Consumer Reports noted in its State of the Net report that 7.5 million children under the age of thirteen have Facebook accounts, and 5 million of these children are under the age of ten.”).

See James Grimmelmann, Saving Facebook, 94 Iowa L. Rev. 1137, 1140 (2009).


See, e.g., Data Use Policy: Sharing and Finding You on Facebook, supra note 109 (explaining that even if you hide your birthday, people may determine when it is if a friend posts a birthday message on your timeline).


Id.


See id.


See Foursquare Labs, Inc. Privacy Policy, supra note 132.

See Kate Murphy, Web Photos that Reveal Secrets, Like Where You Live, N.Y. Times, Aug. 12, 2010, at B6; How are You Doing This?, supra note 134.

How Are You Doing This?, supra note 134.

See id.; Valli & Hannay, supra note 136.

See Murphy, supra note 142.

Valli & Hannay, supra note 136.


See Fursland, supra note 17, at 21; Luscombe, supra note 148.

See Murphy, supra note 142; Child Welfare Info. Gateway, supra note 13, at 11.

See Luscombe, supra note 148, at 46.


See Judith S. Gediman & Linda P. Brown, BirthBond: Reunions Between Birthparents and Adoptees - What Happens After 50-51 (1989) (discussing many different types of information that adoptees may not know about their birth family and history).

See Eldridge, supra note 153, at 203-204.


See Gediman & Brown, supra note 154, at 99-100.

See id. at 186, 190 (noting that siblings may have reunions when a birth parent refuses to meet).

See, e.g., Eldridge, supra note 153, at 208-09 (“I found out my birth mother doesn't even know when my birthday is. . . . I am disappointed that this is not turning out to be a mountaintop experience.”).


See Fursland, supra note 17, at 29.

See Gediman & Brown, supra note 154, at 51.

See Eldridge, supra note 153, at 208-09; Gediman & Brown, supra note 154, at 51.

See, e.g., Eldridge, supra note 153, at 208-09 (“I am disappointed . . . . I am realizing the reality of the rejection of thirty-five years ago. I felt like a stranger-like I don't belong.”).


See, e.g., 2012 Fla. Laws 2035 (“For the purposes of injunctions for protection against stalking under this section, the offense of stalking shall include the offense of cyberstalking.”); cf. Cal. Penal Code § 646.9(g) (West 2010) (including in the offense of stalking threats that are “performed through the use of an electronic communication device”).


See Merritt Baer, Cyberstalking and the Internet Landscape We Have Constructed, 15 Va. J.L. & Tech. 153, 171 (2010). Baer discusses the need to create the right remedies for cyberstalking and other crimes of Internet-introduced harm, “with the recognition that the Internet is not merely a new medium for speech; it is a space in which actions occur. . . . Creating effective cyberstalking statutes will force us to think about where we want the limits of free speech online, and how well we understand the kinds of harms that exist on and because of the Internet.” Id. See also Naomi Harlin Goodno, Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws, 72 Mo. L. Rev. 125, 125-26 (2007) (providing examples of cyberstalking and comparing cyberstalking to stalking); Jacqueline D. Lipton, Combating Cyber-Victimization, 26 Berkeley Tech. L.J. 1103, 1111 (2011) (noting that some jurisdictions require a credible threat to the victim for there to be a cyberstalking violation and that cyberstalking is more likely than traditional stalking to result in severe and immediate emotional or physical harm); Nisha Ajmani, Comment, Cyberstalking and Free Speech: Rethinking the Rangel Standard in the Age of the Internet, 90 Or. L. Rev. 303, 304-05 (2011) (describing cyberstalking as including sending numerous harassing or threatening e-mails to another person, creating
a webpage to threaten or harass another person, encouraging third parties to stalk or harm another person, and intimidating another person via an online chat system).


See, e.g., id. at 13 (describing how one birth mother's fears over psychologically harming her son, who was the adoptee's half-brother, caused her to wait to meet the adopted child).

See, e.g., Luscombe, supra note 43, at 46; Heussner, supra note 43.

See, e.g., Gediman & Brown, supra note 154, at 105 (describing one husband's inability to forgive his wife for becoming pregnant before they met and never telling him about the child).

See, e.g., id. at 204 (explaining how a birth mother's spouse may feel threatened by an adoptee's contact).

Compare id. at 188 (asserting that a large birth family can be welcoming to an adoptee), with id. at 204 (explaining how threatening a reunion can be to a spouse due to feelings of exclusion).


See, e.g., Luscombe, supra note 43, at 46 (“‘Biological parents have called me in tears and in fear’ about being discovered, says Chuck Johnson, acting CEO of the National Council for Adoption . . . . ‘They don't know what to do.’”); Heussner, supra note 43 (explaining how an adoptee's contact with a birth mother was clearly unwanted).

See, e.g., Restatement (Second) of Torts §§ 558-59 (1977); Restatement of Torts § 574 (1938).


All names in this hypothetical are fictitious and do not relate to any real people.

Restatement (Second) of Torts § 558.

Id. § 559.

The Restatement of Torts had a specific defamation tort, “slanderous imputations of unchastity,” for which special harm did not need to be proven, meaning that such statements were per se defamatory. Restatement of Torts § 574. The Restatement states that “[o]ne who falsely and without a privilege to do so, publishes a slander which imputes to a woman unchastity is liable to her.” Id. The Restatement provides two illustrations of situations where the tort might come into play, the second of which was: “A, falsely and without a privilege, states to B that C's child was conceived before her marriage. A is liable to C.” Id. § 574 cmt. b, illus. 2. This tort is not included in the Restatement (Second) of Torts, but a more specific form of that tort is included in section 574, which provides that slanderous imputations of sexual misconduct are slander per se: “One who publishes a slander that imputes serious sexual misconduct to another is subject to liability to the other without proof of special harm.” Restatement (Second) of Torts § 574. Is having a child out of wedlock “serious sexual misconduct”? In the twenty-first century, it cannot credibly be argued that it is.

Restatement (Second) of Torts § 577.

See, e.g., Veilleux v. NBC, 206 F.3d 92, 107 (1st Cir. 2000).

See Martin v. City of Struthers, 319 U.S. 141, 143 (1943).

Compare N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964) (holding that a public official may not recover for statements made regarding public concern unless the public official proves actual malice), with Gertz v. Robert Welch, Inc., 418 U.S. 323, 345 (1974) (holding that a private person warrants greater protection than public officials and public figures). There is no liability for “a false and defamatory communication concerning a public official or public figure in regard to his conduct, fitness or role in that capacity” unless the defendant knows the statement is false and defamatory or acts in reckless disregard of its truth or falsity. Restatement (Second) of Torts § 580A.

Restatement (Second) of Torts § 580B.

Paterson v. Little, Brown & Co., 502 F. Supp. 2d 1124, 1133 (W.D. Wash. 2007) (citing Ward v. Painters' Local Union No. 300, 252 P.2d 253, 256-57 (Wash. 1953)). See also Restatement (Second) of Torts § 581A (“One who publishes a defamatory statement of fact is not subject to liability for defamation if the statement is true.”).


See Restatement (Second) of Torts § 558(b).


See Restatement (Second) of Torts § 600.

Id. § 594.

Id. § 594 cmt. d.

Id.

Id. § 597.

See Haralambie, supra note 4, at 764-65 (discussing adoption generally).

See Restatement (Second) of Torts § 595.

Id.

Id. § 594(2)(b).


See, e.g., Fessler, supra note 206, at 257.

Restatement (Second) of Torts § 596.


Restatement (Second) of Torts § 599.

Id. § 599 cmt. a.

Id. § 603.
Id. § 603 cmt. a.

Id. § 605A.

Id. § 605A cmt. a.


Gitlow v. New York, 268 U.S. 652, 666 (1925) (“For present purposes we may and do assume that freedom of speech and of the press—which are protected by the First Amendment from abridgment by Congress—are among the fundamental personal rights and ‘liberties’ protected by the due process clause of the Fourteenth Amendment from impairment by the States. We do not regard the incidental statement in Prudential Ins. Co. v. Cheek, 259 U.S. 530, 543, that the Fourteenth Amendment imposes no restrictions on the States concerning freedom of speech, as determinative of this question.”) (footnote omitted).


See Restatement (Second) of Torts § 652D (laying out the elements of the tort, which do not include false statements).


Restatement (Second) of Torts § 652D.

Id. § 652D cmt. a.

Id.


Difference Between Electronic/Print Media and Social Media, Firebrand Social Media Blog (Sept. 6, 2012), http://www.firebrandsocialmedia.com/opinions/differencebetween-electronicprint-media-and-social-media/. But see Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 43-44 (Minn. Ct. App. 2009) (holding that posting private medical information on a publicly accessible webpage constitutes publicity). The concurring opinion stated that the holding was too broad, noting that “[n]ot all Internet sites are intended to disseminate information to large numbers of persons. Some information on the Internet consists of communication that is private in nature. One of the primary purposes of social-networking web sites is to allow people to communicate with friends and acquaintances.” Id. at 52 (Johnson, J., concurring).


See Lindsay S. Feuer, Note, Who is Poking Around Your Facebook Profile?: The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites, 40 Hofstra L. Rev. 473, 487-88 (2011).

See Patricia Sanchez Abril, Recasting Privacy Torts in a Spaceless World, 21 Harv. J.L. & Tech. 1, 23 (2007) (“[I]n the culture of cyberspace, no matter how private a topic is traditionally considered, there may be no such thing as unequivocally private subject matter. This seeming evolution in privacy norms evidences the difficulty of the Restatement's reliance on classifying certain subjects as per se private.”).


Cf. id. at 468-69 (noting that adoptive parents have a much smaller interest in the sealed records debate but recognizing that if birth parents obtain access to the adoption records of the children they surrendered, then they may “unreasonably interfere with the lives” of the adoptive parents and their child).

See generally id. at 465-68 (discussing the evolution of the open records debate from the end of World War II to present day).

Restatement (Second) of Torts § 652D cmt. c (1977).

See Sanchez Abril, supra note 229, at 11 (“As technology evolves, social behavior and ensuing privacy harms, as well as people's tolerance of these harms, change.”); Feuer, supra note 228, at 512 (“It is inconsistent with the Fourth Amendment to impose a warrant requirement when individuals are knowingly disclosing their information to 'friends' on Facebook”).

See Fleming, supra note 231, at 465.


See Jeanne A. Howard et al., Evan B. Donaldson Adoption Inst., For the Records II: An Examination of the History and Impact of Adult Adoptee Access to Original Birth Certificates 20-21 (July 2010), http://www.adoptioninstitute.org/publications/7_14_2010_ForTheRecordsII.pdf. According to the report:

Secrecy is a response to events or circumstances that we do not want others to find out about; in the words of Pertman (2000), “We keep secrets about things we're ashamed of or embarrassed about.” Adoptees sometimes feel that something about their very being caused the adoption. The secrecy surrounding confidential, or closed, adoptions reinforces this belief and intensifies consequent feelings of shame and guilt . . . .

. . . .

Advocates argue that sealing birth certificates has placed adoptees in a position of inequality and powerlessness to gain basic information that all other Americans possess. Barring them from accessing facts about their origins accentuates their difference from others and perpetuates shame or a sense of “being lesser.” Adopted individuals are frequently put in the position of explaining this difference, such as when they go to a doctor's office and are asked questions about their medical history or when their children ask questions about their nationality for a school project. On many levels, secrecy and the mystery surrounding confidential adoption create ongoing negative messages or experiences related to being unlike the rest of the world.

Id.

Restatement (Second) of Torts § 652D special note. See also Marc A. Franklin, The Origins and Constitutionality of Limitations on Truth as a Defense in Tort Law, 16 Stan. L. Rev. 789, 834 (1964) (“[D]espite occasional harm to an individual, . . . true statements are in the best interest of society and should be broadly protected.”); Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 Geo. L.J. 2381, 2392 (1996) (noting that although the disclosure tort is a viable cause of action in about thirty-five states, plaintiffs rarely succeed because it is treated as “a battle between First Amendment values and an inchoate, elastic privacy ‘right’”); Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan. L. Rev. 1049, 1122 (2000) (arguing that in general, speech that reveals personal information may be constitutionally restricted only under express or implied contract).

Sanchez Abril, supra note 229, at 45.

372 S.E.2d 711 (N.C. 1988).

Id. at 712.

Id. at 713.

Id. at 714 (citing Frederick Davis, What Do We Mean By “Right to Privacy”? 4 S.D. L. Rev. 1, 4 (1959)).

Hall, 372 S.E.2d at 717; accord Anderson v. Fisher Broad. Co., 712 P.2d 803, 814 (Or. 1986). The Supreme Court of Oregon, declining to rule on the constitutional issue, held:
The truthful presentation of facts concerning a person, even facts that a reasonable person would wish to keep private and that are not ‘newsworthy,’ does not give rise to common-law tort liability for damages for mental or emotional distress, unless the manner or purpose of defendant’s conduct is wrongful in some respect apart from causing the plaintiff’s hurt feelings.

See 372 S.E.2d at 717.


See Restatement (Second) of Torts § 652B cmt. a (1977).


See Restatement (Second) of Torts § 652B cmt. a (1977).

Tigran Palyan, Common Law Privacy in a Not So Common World: Prospects for the Tort of Intrusion upon Seclusion in Virtual Worlds, 38 Sw. L. Rev. 167, 180 (2008) (stating that the “affirmative act” element is “satisfied through an interference that is physical or trespassory” in a majority of cases).

Restatement (Second) of Torts § 652B cmt. c.

Tigran Palyan, Common Law Privacy in a Not So Common World: Prospects for the Tort of Intrusion upon Seclusion in Virtual Worlds, 38 Sw. L. Rev. 167, 180 (2008) (stating that the “affirmative act” element is “satisfied through an interference that is physical or trespassory” in a majority of cases).

Id. § 652B.

Tigran Palyan, Common Law Privacy in a Not So Common World: Prospects for the Tort of Intrusion upon Seclusion in Virtual Worlds, 38 Sw. L. Rev. 167, 180 (2008) (stating that the “affirmative act” element is “satisfied through an interference that is physical or trespassory” in a majority of cases).

See, e.g., Fursland, supra note 17, at 45, 47-48 (noting that Facebook users can block individual people); Amanda Lenhart et al., Teens and Social Media 13 (Dec. 19, 2007), http://www.pewinternet.org/°/ media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf. (“Two-thirds (66%) of teens with an online profile say they restrict access to it in some way . . . .”).

Sanchez Abril, supra note 229, at 5. But see Diane Leenheer Zimmerman, The “New” Privacy and the “Old”: Is Applying the Tort Law of Privacy Like Putting High-Button Shoes on the Internet?, 17 Comm. L. & Pol'y 107, 114 (2012) (arguing that there are fundamental reasons that “the tort regime governing policy has the shape it does” and that, even with technological change, the “center holds”).

Perhaps the most sweeping is the suggestion that we integrate the English confidentiality tort into American privacy law. See Neil M. Richards & Daniel J. Solove, Privacy's Other Path: Recovering the Law of Confidentiality, 96 Geo. L.J. 123, 180-82 (2007).


See, e.g., Andrew J. McClurg, A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 Nw. U. L. Rev. 63, 143 (2003) (“[A]ppropriation tort provides an appropriate vehicle for restoring a just balance in the autonomy-control equation between individuals and businesses who seek to profit from their individuality.”).


277 U.S. 438 (1928).

See id. at 478 (Brandeis, J., dissenting).

See Paul v. Davis, 424 U.S. 693, 713 (1976) (“In these areas it has been held that there are limitations on the States' power to substantively regulate conduct.”).
See Eugene C. Rich et al., Reconsidering the Family History in Primary Care, 19 J. Gen. Internal Med. 273, 273 (2004), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1492151/pdf/jgi_30401.pdf (“The patient's family history remains a critical element in risk assessment for many conditions.”); Liesbeth Claassen et al., Using Family History Information to Promote Healthy Lifestyles and Prevent Diseases: A Discussion of the Evidence, BMC Pub. Health (May 13, 2010), http://www.biomedcentral.com/1471-2458/10/248 (“In addition to risk assessment, family history information can also be used to personalize health messages, which are potentially more effective in promoting healthy lifestyles than standardized health messages.”).

See Claassen et al., supra note 264 (noting that susceptibility genes for common chronic diseases are “newly discovered each day”).


See Howard, supra note 238, at 19 (quoting Dr. Aubrey Milunsky, Director of the Center for Human Genetics at Boston University School of Medicine, about adoptees who do not know their family medical history). Dr. Milunsky explains: “It is really important to know your family history if you are to secure your health or the health of your children or even to save your life or the lives of your children.” Id.


Howard, supra note 238, at 25-26.

See generally Judith A. Seltzer & Suzanne M. Bianchi, Children's Contact with Absent Parents, 50 J. Marriage & Fam. 663, 663, 667 (Aug. 1988) (discussing the ties between children and their biological parents and how these ties are affected when a child does not live with a biological parent); Biology Online, http://www.biology-online.org/dictionary/Parent (last visited Dec. 22, 2012) (defining “parent” as “one who begets, or brings forth, offspring; a father or a mother”).


See id.


See id.

See id.


See Lothar Determann, Social Media Privacy: A Dozen Myths and Facts, 2012 Stan. Tech. L. Rev. 7, 3 (2012), http://stlr.stanford.edu/pdf/determann-socialmediaprivacy.pdf. Determann calls the idea that people own personal data about themselves a myth and states the following: Talk about informational self-determination and proposals for property law regimes to protect privacy sometimes gives people the idea that they own personal data about themselves. Fact is that no one owns facts. Factual information is largely excluded from intellectual property law protection: copyright law protects only creative expression, not factual information. Trade secret law protects information that companies keep secret if such information derives an economic value from being secret. Personal information about you that you or others post on social media platforms, however, is not secret and thus not subject to trade secret law protection. When social media companies aggregate information about usage and user preferences, the social media companies can claim trade secret ownership rights in such aggregate information, but they own such trade secrets and you do not. Also, databases with content and personal information can be protected under European database laws and U.S. state laws on appropriation, but again, as property of the social media companies and not as your personal property. So, if anyone owns personal data about you, it is the social media companies, not you.

Id. (footnotes omitted).


See How Parents Use Facebook to Keep Tabs on Their Kids, supra note 290 (indicating that 24% of parents use Facebook to spy on their children because it is the only way to see what their children are doing).


See Powell, supra note 280.