

# Catholic University Journal of Law and Technology

---

Volume 26 | Issue 1

Article 7

---


2018

## Dating Dangerously: Risks Lurking within Mobile Dating Apps

Alyssa Murphy

*Catholic University of America (Student)*

Follow this and additional works at: <https://scholarship.law.edu/jlt>

 Part of the [Communications Law Commons](#), [Internet Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

---

### Recommended Citation

Alyssa Murphy, *Dating Dangerously: Risks Lurking within Mobile Dating Apps*, 26 Cath. U. J. L. & Tech 100 (2017).

Available at: <https://scholarship.law.edu/jlt/vol26/iss1/7>

This Comments is brought to you for free and open access by CUA Law Scholarship Repository. It has been accepted for inclusion in Catholic University Journal of Law and Technology by an authorized editor of CUA Law Scholarship Repository. For more information, please contact [edinger@law.edu](mailto:edinger@law.edu).

---

## DATING DANGEROUSLY: RISKS LURKING WITHIN MOBILE DATING APPS

Alyssa Murphy<sup>+</sup>

Looking for love has never been easy, but in the twenty-first century, it has become dangerous.<sup>1</sup> Mobile dating applications (“apps”) have taken over the way young people meet by connecting strangers, not based on commonalities, but rather by their location.<sup>2</sup> The dating apps have quickly risen in popularity<sup>3</sup> and frequently result in new relationships,<sup>4</sup> but the number of crimes committed due to connections made through the apps has increased as well.<sup>5</sup> For example,

---

<sup>+</sup> J.D. Candidate, May 2018, The Catholic University of America Columbus School of Law; B.A., Political Science, James Madison University, 2015. I would like to extend a special thank you to Professor Mary Graw Leary for her insight and guidance in the research and writing of this Comment. I would also like to thank my family and friends for their thought-provoking contributions, and endless support.

<sup>1</sup> See Vanessa Borge, *The Dangers Of Looking For Love Online*, CBS MIAMI (June 11, 2015, 11:01 PM), <http://miami.cbslocal.com/2015/06/11/the-dangers-of-looking-for-love-online/>. See also Aaron Smith & Maeve Duggan, *Online dating & Relationships*, PEW RESEARCH 2 (Oct. 21, 2013), <http://www.pewinternet.org/2013/10/21/online-dating-relationships/> (explaining that since 2005, online daters are more likely to meet people they have met online for dates).

<sup>2</sup> Theo Miller, *How Tinder Became A Gateway Dating App*, FORBES (Aug. 7, 2017, 1:30 PM), <https://www.forbes.com/sites/theodorecasey/2017/08/07/how-tinder-became-a-gateway-dating-app/#6e1b6eb739b5>. See generally *Privacy Policy*, TINDER, <https://www.gotinder.com/privacy> (last visited Dec. 19, 2017) (stating that a user’s geographic location is collected while the application is running); *Privacy Policy*, BUMBLE, <https://bumble.com/en-us/privacy> (last visited Dec. 19, 2017) (listing how geolocation is used by the application to offer certain features to the users and informing the user that despite disabling location services, Bumble can still determine a user’s city, state, and country location).

<sup>3</sup> See generally *Online Dating Statistics*, STAT. BRAIN (May 12, 2017), <http://www.statistic-brain.com/online-dating-statistics/> (showing up to date statistics regarding online dating including numbers of users and percentage of successful relationships).

<sup>4</sup> See generally *id.*

<sup>5</sup> *Crimes Linked to Tinder and Grindr Increase Seven Fold*, TELEGRAPH (Mar. 16, 2016, 12:55 PM), <http://www.telegraph.co.uk/news/2016/03/16/crimes-linked-to-tinder-and-grindr-increase-seven-fold/>.

in 2016, the body of Preston Talley was found in Brooksville, Florida.<sup>6</sup> Investigators later learned that one of Talley's killers, Kayla Morrow, a potential partner he met through a mobile dating app, lured him to a secluded area using sex and methamphetamine.<sup>7</sup> Three men were awaiting the pair's arrival and proceeded to beat Talley to death with a baseball bat.<sup>8</sup> Law enforcement officials were able to apprehend all four individuals. Each was subsequently charged with first-degree murder.<sup>9</sup> Unfortunately, this example is the exception, not all perpetrators are caught.<sup>10</sup>

Globally, and specifically in the United States, millions of people of all ages have begun using mobile dating apps.<sup>11</sup> For example, Tinder, one of the most popular dating apps, hosts over 50 million users worldwide.<sup>12</sup> Online dating, and more specifically mobile online dating, has increased for all ages over the past two years.<sup>13</sup> Young millennials favor mobile dating as a predominant form of dating because they are more likely to own a Smartphone than other members of the population.<sup>14</sup> Dating apps have become the normal way to date and to get to know each other; it is therefore unsurprising the amount of dating apps available for download has increased in the past several years as well.<sup>15</sup> Some of the most commonly used dating apps explored in this Comment include Tinder, Bumble, Grindr, and Hinge.<sup>16</sup>

One similarity employed by all of these dating apps is the active proximity-based location system.<sup>17</sup> Proximity-based systems continuously broadcast and

---

<sup>6</sup> Abraham Rinquist, *10 Dating App Murders*, LISTVERSE (Nov. 26, 2016), <http://listverse.com/2016/11/26/10-dating-app-murders/>.

<sup>7</sup> Rinquist, *supra* note 6.

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> See generally Erika Borrajo, Manuel Gámez-Guadix & Esther Calvete, *Justification Beliefs of Violence, Myths about Love and Cyber Dating Abuse*, 27 PSICOTHEMA 327, 331 (2015) (describing the rise of cyber abuse among young individuals).

<sup>11</sup> Kevin Murnane, *Report Shows More People of All Ages Are Dating Online*, FORBES (Mar. 2, 2016, 6:15 PM), <https://www.forbes.com/sites/kevinmurnane/2016/03/02/pew-report-who-uses-mobile-dating-apps-and-online-dating-sites/#8194fc966e30> ("Online dating appears to have increased for almost every age group over the past two years.").

<sup>12</sup> Nick Bilton, *Tinder Taps an Age-Old Truth*, N.Y. TIMES, OCT. 30, 2014, at E1.

<sup>13</sup> Murnane, *supra* note 11.

<sup>14</sup> *Id.*

<sup>15</sup> *The 8 Best dating Apps for 2017*, DIGITAL TRENDS (Aug. 11, 2017, 9:24 AM), <http://www.digitaltrends.com/mobile/best-dating-apps/>. See also Murnane, *supra* note 11.

<sup>16</sup> See generally Nathan McAlone, *RANKED: America's most popular dating apps from best to worst*, BUS. INSIDER (Feb. 11, 2016, 12:22 PM), <http://www.businessinsider.com/the-best-and-worst-dating-apps-in-2016-ranked-by-reviews-2016-2/#no-5-tinder-395100-7> (ranking dating apps with over 2,000 reviews to determine which were meeting user expectations).

<sup>17</sup> Jody Farnden, Ben Martini & Kim-Kwang Raymond Choo, *Privacy Risks in Mobile*

track a user's location to help facilitate meeting people nearby.<sup>18</sup> But the sharing and storage of such intimate and private information on the app, whether purposely given by the user or not, raises concerns about the user's privacy and safety.<sup>19</sup> Based on this feature, predators lurking in the digital shadows of the dating apps can ascertain a user's address, view their movements throughout the day and eventually, virtually stalk a user.<sup>20</sup> They can do so by monitoring and keeping track of the user's location when he or she indicates he or she is at home, at work, or elsewhere, by noting how many miles away the users are from each other at that time.<sup>21</sup> The constant tracking allows dangerous users to reconstruct daily patterns of their prey.<sup>22</sup> As a result, the inherent characteristics of these modern apps coax unscrupulous users into exploiting potential lovers.<sup>23</sup> Coupled with the lack of restrictions on a user's ability to access personal information, this free flow of information opens the door to dangers associated with a lax in privacy protections and worse, the dangers associated with acts of violence facilitated by the app.<sup>24</sup> But once an infringement on intimate, personal information has occurred, or an act of violence has taken place associated with a mobile dating app, what information can be accessed in order to catch the culprit red-handed, or in this reality, phone-in-hand?

This alarming reality raises the issue of what data can actually be accessed in the assistance of prosecuting crimes associated with the apps without infringing on user's privacy interests any more than mobile dating apps already do. Recent case studies have used forensic techniques on popular proximity-based dating apps in order to determine the types of data that can be recovered from user's devices.<sup>25</sup> These studies have revealed the types of information available for recovery from mobile dating apps:

[t]hrough network traffic monitoring we were able to collect profile pictures, chat, nearby users, user profile and device information. A preview of the last message sent or received from each user can be viewed, but not historical messages. The users [sic] profile is recoverable, along with a list of users they have declared as a

---

*Dating Apps 1* (2015) Proceedings of the 21st Americas Conference on Information Systems, Conference in Puerto Rico 13-15, <https://arxiv.org/pdf/1505.02906.pdf>.

<sup>18</sup> *Id.* at 1-2.

<sup>19</sup> *Id.* at 2.

<sup>20</sup> *Id.*

<sup>21</sup> *Id.* at 6.

<sup>22</sup> See generally Doug Gross, *How Your Movements Create a GPS Fingerprint*, CNN (Mar. 26, 2013, 2:39 PM), <http://www.cnn.com/2013/03/26/tech/mobile/mobile-gps-privacy-study/index.html> (showing how location data can be used to predict the behaviors of an individual).

<sup>23</sup> See generally Farnden, *supra* note 17, at 2 (describing how data from mobile dating apps are being used in not only traditional crimes but also cybercrimes).

<sup>24</sup> *Id.* at 2.

<sup>25</sup> *Id.* at 5.

'match.'<sup>26</sup>

Under the Fourth Amendment to the United States Constitution, courts have determined the government must obtain a warrant, stated with particularized facts that are sufficient to indicate the data to be searched from a cell phone.<sup>27</sup> This data inherently includes information stored on mobile dating apps.<sup>28</sup> However, obtaining a warrant is not troublesome for law enforcement officers, including prosecutors, when there is a showing, supported by probable cause, that data stored on mobile dating apps aids in apprehension or conviction of the offender.<sup>29</sup>

This Comment will discuss the importance of finding a delicate balance between privacy interests associated with using modern mobile dating apps and the need for user protection from heinous crimes. In prosecuting these crimes, users must be willing to relinquish their private information in exchange for justice. Part I will explain and breakdown the dating apps, including how they work and how they are used, in order to give a comprehensive understanding of the characteristics that lead to poignant criticism of the apps. Part II will briefly explore the types of crimes that typically stem from mobile dating apps including solicitation, stalking, murder, and human trafficking. Part III will address the privacy risks exposed by the apps, specifically focusing on the types of information that is retrievable from a mobile dating app. This section will address the differences in the data that comprises a location record and data that concerns intimate messages and other stored information from the apps. Lastly, Part IV will analyze the legal implications specific to a search of data stored in mobile dating apps under the Fourth Amendment. Namely, it will address the scope of a search warrant granting the search of a cell phone and emphasize the importance of describing with particularity the data to be searched. Part IV will argue that obtaining a warrant for intimate information, aside from geolocation data, should not be a hurdle for the prosecution. Achieving justice for victims of crimes associated with mobile dating apps substantially outweighs the potential infringement on the user's privacy with a limited scope.

## BREAKDOWN OF THE APPS

---

<sup>26</sup> *Id.*

<sup>27</sup> *Riley v. California*, 134 S. Ct. 2473, 2485 (2014).

<sup>28</sup> *Id.*

<sup>29</sup> *Warden v. Hayden*, 387 U.S. 294, 306-07 n.11 (1967) ("Government may demonstrate probable cause and lawfully search for stolen property even though the true owner is unknown or unavailable to request and authorize the Government to assert his interest. As to instrumentalities, the Court in *Gouled* allowed their seizure, not because the Government had some property interest in them (under the ancient, fictitious forfeiture theory), but because they could be used to perpetrate further crime.").

### A. The Logistics: How to Use Modern Mobile Dating Apps

Tinder has over 50 million members with about 10 million members who are active every day.<sup>30</sup> Tinder is one of the biggest and most widely used dating apps of the twenty-first century.<sup>31</sup> Tinder and other similar dating apps use Facebook users' accounts in order to set up basic elements of the dating profile.<sup>32</sup> Once logged in and linked through Facebook, Tinder users answer several questions specific to intimate preferences such as sexual orientation, age demographics, and the distance the user is willing to travel to meet up with his or her partner.<sup>33</sup> In setting up the basic profile, users can add and rearrange photos already linked to the Tinder account through the user's Facebook profile.<sup>34</sup>

The user has several positive benefits by linking a user's Facebook profile to his or her Tinder account. Overall, Facebook, as a single entity is considered safe.<sup>35</sup> Facebook ensures that profiles viewed on Tinder are real by removing fake profiles from the site.<sup>36</sup> Since Facebook and Tinder associate and share the user's photos, users can save time editing or updating his or her dating app by allowing the app to pull the user's latest photos he or she has added to Facebook.<sup>37</sup> The most favorable aspect of the link between Tinder and Facebook is that a user can see what friends they have in common with a potential match on the dating app.<sup>38</sup> This crucial detail allows users to feel like they can authenticate the potential lover before meeting in real life to provide assurance that a user is not falling prey to a trap like Preston Talley.<sup>39</sup>

Besides being able to link a user's account to his or her Facebook profile, another reason Tinder's popularity is burgeoning is the "swipe" feature.<sup>40</sup> The act of swiping, or moving a finger from one side of the phone screen to the other, on someone's profile indicates whether someone is interested in the person.<sup>41</sup> The app presents users with a snapshot of potential "matches" based on photos and other information in a person's profile.<sup>42</sup> If the user is uninterested, he or she can swipe left.<sup>43</sup> Conversely, if the user is interested in starting a conversation

---

<sup>30</sup> Christen Costa, *How Does Tinder Work? What Is Tinder?*, GADGET REV. (Dec. 30, 2016), <http://www.gadgetreview.com/how-does-tinder-work-what-is-tinder>.

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

<sup>39</sup> Rinquist, *supra* note 6.

<sup>40</sup> Costa, *supra* note 30.

<sup>41</sup> *Id.*

<sup>42</sup> *See id.*

<sup>43</sup> *Id.*

with that person, he or she can swipe right.<sup>44</sup> The “match” terminology stems from the users both swiping right on each other’s profiles.<sup>45</sup> Users are limited in their number of swipes per day, regardless of which direction.<sup>46</sup> However, premium versions of these apps, specifically Tinder, allow the user to make more swipes per day.<sup>47</sup> Once matched, users can enter into a screen resembling a chat room or text message configuration in which either partner can initiate a conversation.<sup>48</sup> However, the more information users are willing to share on his or her Tinder profile, the higher the risks are for privacy infringements and susceptibilities to crimes like stalking.<sup>49</sup> For example, with permission, users can link their Instagram accounts to their Tinder profiles so other users have greater access to photos and private information.<sup>50</sup> Another form of information that can be shared by the user’s account, so long as their phone is powered on, is a steady stream and record of the user’s geolocation.<sup>51</sup>

### B. Geolocation: The Crux of Mobile Dating Apps

The ubiquitous use of geolocation tracking on Tinder and similar mobile dating apps allows users to always know who is nearby and available to meet without traveling far from the user’s position.<sup>52</sup> Geolocation technology refers to the process of determining the position of a user’s mobile device; the position itself is called the geolocation and modern mobile dating apps could not function without it.<sup>53</sup> Geolocation information increases the functionality of the app and is convenient for users searching for a partner from the comfort of their homes – an attractive component of all mobile dating apps.<sup>54</sup> The position is determined by the user’s latitude and longitude on a traditional map and that information is frequently related to original Global Positioning System (“GPS”) information and technology.<sup>55</sup> Such services are today called Location Based Services and

---

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

<sup>46</sup> *Id.*

<sup>47</sup> *Id.*

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*

<sup>50</sup> *Id.*

<sup>51</sup> *Always Be Oriented with the Integration of Geolocation into Your App*, CLEVEROAD (Feb. 4, 2016), <https://www.cleveroad.com/blog/always-be-orientated-with-the-integration-of-geolocation-into-your-app>.

<sup>52</sup> Costa, *supra* note 30.

<sup>53</sup> *Always Be Oriented with the Integration of Geolocation into Your App*, *supra* note 51.

<sup>54</sup> *Id.*

<sup>55</sup> Daniel Ionescu, *Geolocation 101: How It Works, the Apps, and Your Privacy*, PCWORLD (Mar. 29, 2010, 7:45 PM), <http://www.pcworld.com/article/192803/geolo.html>.

are accessible on all mobile devices with GPS tools.<sup>56</sup> Since the app keeps updating and continually tracks the user's geolocation, it is feasible and preferred that the pool of potential matches changes as the user's location changes.<sup>57</sup>

Although all mobile dating apps use various Location Based Services, they are not all "created equal."<sup>58</sup> Some geolocation technologies are slower than others and therefore do not provide the best routes for modern mobile daters.<sup>59</sup> Most Smartphones employ a Wi-Fi network proximity system to coordinate user's geolocation, even while indoors.<sup>60</sup> This technology analyzes the names and addresses of Wi-Fi networks nearby, allowing the app to ascertain exactly where the user is located by pinpointing Wi-Fi networks to which the phone is close enough to connect.<sup>61</sup> A hybrid system such as this, which combines Wi-Fi proximity with GPS coordinates, is the best and most reliable indicator of a user's location at any given time.<sup>62</sup> Without this accuracy, users would experience greater hurdles finding companionship on mobile dating apps.<sup>63</sup>

### C. An Explosion of Mobile Dating Apps

Other mobile dating apps follow Tinder's example by successfully harnessing users' geolocation and Facebook profiles as a basis for matches.<sup>64</sup> Bumble, a close competitor of Tinder, operates in logistically the same way as its larger

---

<sup>56</sup> *Id.*

<sup>57</sup> Costa, *supra* note 30.

<sup>58</sup> McAlone, *supra* note 16.

<sup>59</sup> See Jack Cox, *Using Geolocation Technology to Improve Customer Experience – Another Lesson from the Mobile World of Pokémon Go*, CAPTECH (Sept. 26, 2016), <https://www.capttechconsulting.com/blogs/geolocation-technology-improve-customer-experience-lesson-mobile-world-pokemon-go> (discussing other location technologies that other popular apps use).

<sup>60</sup> Larry Greenemeier, *A Positioning System that Goes Where GPS Can't*, SCI. AM. (Jan. 23, 2008), <https://www.scientificamerican.com/article/indoor-positioning-system/>.

<sup>61</sup> See Marie Black, *What Is Bumble? Bumble Dating App FAQ*, TECHADVISOR (Dec. 12, 2014), <http://www.techadvisor.co.uk/feature/software/what-is-bumble-bumble-dating-app-faq-3590386/> (showing how distance can affect matches on Bumble).

<sup>62</sup> Fred Zahradnik, *An Explanation of Wi-Fi Triangulation*, LIFEWIRE (June 12, 2017), <https://www.lifewire.com/wifi-positioning-system-1683343> ("Wi-Fi GPS . . . is particularly useful in urban areas where there are Wi-Fi networks broadcasting all over the place. However, the benefits are even greater when you consider that there are some circumstances where it's simply too difficult for GPS to work, like underground, in buildings or malls where GPS is too weak or intermittent.").

<sup>63</sup> *Id.*

<sup>64</sup> *What Is Bumble Dating App and How Does It Work?*, MY DATING HACKS, <http://my-datinghacks.com/what-is-bumble-dating-app-and-how-does-it-work/> (last visited Dec. 19, 2017).



counterpart—by linking dating profiles with social media accounts like Facebook.<sup>65</sup> However, in this app the woman must be the first to message her match.<sup>66</sup> With this feature, Bumble hoped to reduce the number of inappropriate messages initiated by men, therefore granting women a little more protection from unwanted communications.<sup>67</sup>

Still, Bumble, like Tinder, borrows users' profile pictures from Facebook and users' "age, location, job title, and educational background."<sup>68</sup> Users of Bumble, like users of other dating apps, are cognizant that private information like this will be visible to all users of the app when they sign up.<sup>69</sup> Nevertheless, they bear the risk of other users taking advantage of this free-flow of information.<sup>70</sup> Unique to Bumble, matches formed as a result of mutual "right-swipes" expire after twenty-four hours of the match.<sup>71</sup> A failure on behalf of the woman to initiate conversation gives the man an option to extend the window of initiation another twenty-four hours.<sup>72</sup> If the woman still does not message the man (or woman in the case of same-sex partnerships), then the match will permanently expire.<sup>73</sup> In a sense, this ensures that current matches are always up-to-date and gives the woman more control of whom she wishes to let into her virtual, and real life.<sup>74</sup>

Another mobile dating app closely modeled after Tinder is Grindr.<sup>75</sup> Grindr is the largest social networking app exclusively targeted toward gay and bisexual men.<sup>76</sup> The app has over two million daily users in over one hundred and ninety-two countries.<sup>77</sup> Setting up a Grindr profile is slightly more in-depth than Tinder or Bumble. Grindr does not gather information from the user's Facebook profile unless the user gives the app permission to link the profiles later on in the setup process.<sup>78</sup> Instead, the user fills in personal information like a display name, headline, age (users must be over the age of eighteen), and a biography comprising of a brief description of interests, hobbies, intentions, and the like.<sup>79</sup> Grindr caters to the gay community by allowing users to identify themselves through

---

<sup>65</sup> *Id.*

<sup>66</sup> *Id.*

<sup>67</sup> Black, *supra* note 61.

<sup>68</sup> *Id.*

<sup>69</sup> *Id.*

<sup>70</sup> *Id.*

<sup>71</sup> *What Is Bumble Dating App and How Does It Work?*, *supra* note 64.

<sup>72</sup> *Id.*

<sup>73</sup> *Id.*

<sup>74</sup> *Id.*

<sup>75</sup> *About*, GRINDR, <https://www.grindr.com/about/> (last visited Dec. 19, 2017).

<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

<sup>78</sup> *How to Use Grindr*, WIKIHOW, <http://www.wikihow.com/Use-Grindr> (last visited Dec. 19, 2017).

<sup>79</sup> *Id.*

“Grindr Tribes.”<sup>80</sup> The gay community uses “tribes” to indicate body type and other physical qualities to guarantee a more realistic match while using the app.<sup>81</sup> For example, the tribe term “Twink” is often used to describe a young college student who is thin in stature.<sup>82</sup> Yet, the tribe term “Bear” refers to someone who is heavier and often has more body hair.<sup>83</sup> By using accepted terminology in the gay community, Grindr allows users to advertise their outward appearance to potential partners.<sup>84</sup>

Unlike Tinder or Bumble, Grindr did not adopt the “swipe” feature as a way to match users with other users.<sup>85</sup> Instead, other users nearby appear on a single screen.<sup>86</sup> From there, users can select other user’s accounts by tapping on the image to enlarge the profile picture and to read more biographical information shared by that user.<sup>87</sup> If the user is not impressed by any options provided on the first screen, the user can scroll down to load more men nearby or to filter the presented men based on individualized preferences such as eyebrow color, arm hair density, and muscle tone.<sup>88</sup> This real-time snapshot into the men located near the user, similar to geolocational snapshots in other apps like Tinder and Bumble, allow the user to be more selective in his communications because there are always new people moving into the same area as the user.<sup>89</sup> The Grindr user, if intrigued, can save potential interests to his “favorites” folder by selecting the star feature. If he chooses, he can start a conversation.<sup>90</sup>

The final mobile dating app this Comment explores is Hinge.<sup>91</sup> Hinge creators wanted to excel and stand out in a world of dating that has been commonly referred to as an “apocalypse.”<sup>92</sup> Mobile dating has adopted this negative stigma because of the abundance of reported unsuccessful relationships attributable to the use of dating apps.<sup>93</sup> As a result, Hinge decided to re-vamp their app with

---

<sup>80</sup> *Id.*

<sup>81</sup> *Id.*

<sup>82</sup> *Id.*

<sup>83</sup> *Id.*

<sup>84</sup> *Id.*

<sup>85</sup> *Id.* (stating that users on Grindr tap on pictures of other users to add potential dates to their favorites).

<sup>86</sup> *Id.*

<sup>87</sup> *Id.*

<sup>88</sup> *Id.*; Kris Seto, *18 Ground Rules for Grindr*, HUFFINGTON POST (Oct. 7, 2011, 11:13 AM), [http://www.huffingtonpost.com/kris-seto/grindr-rules\\_b\\_977982.html](http://www.huffingtonpost.com/kris-seto/grindr-rules_b_977982.html).

<sup>89</sup> Seto, *supra* note 88.

<sup>90</sup> *How to Use Grindr*, *supra* note 78.

<sup>91</sup> Kristin Tice Studeman, *Hinge, a Dating App, Introduces Friends of Friends*, N.Y. TIMES (Mar. 28, 2014), [https://www.nytimes.com/2014/03/30/fashion/hinge-a-dating-app-introduces-friends-of-friends.html?\\_r=0](https://www.nytimes.com/2014/03/30/fashion/hinge-a-dating-app-introduces-friends-of-friends.html?_r=0).

<sup>92</sup> Margaret Abrams, *Can the New Version of Hinge Actually Change How We Use Dating Apps?*, OBSERVER (Oct. 14, 2016, 11:08 AM), <http://observer.com/2016/10/can-the-new-version-of-hinge-actually-change-how-we-use-dating-apps/>.

<sup>93</sup> *Id.*

hopes of helping users actually meet and find a viable relationship.<sup>94</sup> The app employs tactics similar to Tinder and Bumble in that syncing profiles with the user's Facebook account, mutual friends, and geolocation.<sup>95</sup> However, Hinge takes profiles to the next level by encouraging users to share personal anecdotes and activities ranging from shows the user is watching on Netflix to a go-to list of karaoke songs favored by the user.<sup>96</sup> Instead of swiping, Hinge and Grindr are similar in that nearby choices emerge from a singular screen; it is up to the user to "heart" or "favorite" specific activities the other person enjoys as a means to start a conversation with more substance than merely saying "hey."<sup>97</sup> Hinge also offers a "deal-breaker" feature, which allows users to ignore other users based on certain undesirable characteristics like age or even location if the user is farther than one is willing to travel.<sup>98</sup> Although the intentions of providing more substantive and personal information on the app is arguably good, it raises additional concerns of the user's privacy and threats of exploitation of shared information, for example, if one were to gain access to the information unlawfully.<sup>99</sup>

## CRIMES ASSOCIATED WITH MOBILE DATING APPS

### A. The Environment Created by Mobile Dating Apps Invites Danger

Unfortunately for users trying to find love in the digital age, crimes, including rape, attempted murder, child sex grooming, and various cybercrimes are linked to dating apps like Tinder and Grindr.<sup>100</sup> These dating app crimes have increased seven fold in just two years.<sup>101</sup> The crime rates have become staggeringly high in recent years due to the perpetually growing number of users the apps attract and the geolocation service provided while using the apps.<sup>102</sup> Specifically, the geolocation technology lets the potential assailant know how close he or she is to

---

<sup>94</sup> *Id.*

<sup>95</sup> *Id.*

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

<sup>98</sup> *Id.*

<sup>99</sup> *Id.*

<sup>100</sup> See generally *Grooming Dynamic*, NAT'L CTR. FOR VICTIMS OF CRIME, <https://victimsofcrime.org/media/reporting-on-child-sexual-abuse/grooming-dynamic-of-csa> (last visited Dec. 19, 2017) (describing the methods child predators use on the Internet to establish a trusting relationship that is then used against the victim to break down their defenses and exploit them).

<sup>101</sup> *Crimes Linked to Tinder and Grindr Increase Seven Fold*, *supra* note 5.

<sup>102</sup> *Id.* See also Wendy Saltzman, *Warning About Dating Apps After Recent Violent Crimes*, ABC6 (Apr. 25, 2014, 12:29 AM), <http://6abc.com/archive/9515810/>.

his or her potential victim.<sup>103</sup> Thus, the geolocation feature provides users with an unprecedented ability to find love nearby without leaving the couch, but also exposes the user to unexpected dangers.<sup>104</sup>

Figures and statistics describing the crime rates attributable to connections on mobile dating apps come from police reports that mention dating apps like Tinder or Grindr in the description of the allegation.<sup>105</sup> Any mention of any of these apps does not necessarily mean the apps were used in commission of the crime.<sup>106</sup> However, indirect mentioning of the apps could mean the victim and suspect met on the app or the app was in use at the time of the crime, but the app was not directly related to the crime itself.<sup>107</sup> For example, the United Kingdom reported that offenders committed more than four hundred offenses in connection with dating apps.<sup>108</sup> However, law enforcement fears the intimate nature of the apps lends itself to more crimes going unreported.<sup>109</sup> For instance, closeted as well as openly gay men enjoy the use of Grindr.<sup>110</sup> This knowledge allows perpetrators to target closeted gay or bisexual men because they are less likely to file reports with the police as a means to protect anonymity.<sup>111</sup> An unwillingness to report crimes of this nature out of fear of being recognized as homosexual leaves users in the dark about all of the serious dangers hidden behind the screens of dating apps.

Although the apps do not intend for circumstances of violence to arise, the apps are not equipped to judge whether someone with whom the user is communicating is potentially dangerous.<sup>112</sup> The ease and free-flow of information on the apps make users more open to criminal activity, which in reality, should be horrifying for the user, but the number of daily users across the mobile dating app sphere continues to sky-rocket every day.<sup>113</sup> The recent surge in online and mobile dating has “given rise to a ‘new kind of sexual offender,’” one unique to the digital age.<sup>114</sup> The convenient practice of dating through one’s cell phone has

---

<sup>103</sup> Saltzman, *supra* note 102.

<sup>104</sup> *Id.*

<sup>105</sup> *Crimes Linked to Tinder and Grindr Increase Seven Fold*, *supra* note 5.

<sup>106</sup> *Id.*

<sup>107</sup> *Id.*

<sup>108</sup> *Id.*

<sup>109</sup> *Id.*

<sup>110</sup> *About*, GRINDR, [www.grindr.com/about](http://www.grindr.com/about) (last visited Dec. 19, 2017). *See also Closeted*, MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY (11th ed. 2003) (defining “closeted” as “a state or condition of secrecy, privacy, or obscurity <came out of the [closet]>”).

<sup>111</sup> *Crimes Linked to Tinder and Grindr Increase Seven Fold*, *supra* note 5.

<sup>112</sup> Amanda Connolly, *Tinder and Grindr Are More Dangerous Than Ever*, TNW (Jan. 11, 2016), [https://thenextweb.com/insider/2016/01/11/tinder-and-grindr-are-more-dangerous-than-ever-according-to-uk-report/#.tnw\\_2WIS8Gd0](https://thenextweb.com/insider/2016/01/11/tinder-and-grindr-are-more-dangerous-than-ever-according-to-uk-report/#.tnw_2WIS8Gd0).

<sup>113</sup> *Id.*

<sup>114</sup> Miriam Wells, *Reports of Rape Linked to Online Dating Rise 450 Percent in Five Years*, VICE NEWS (Feb. 8, 2016, 8:35 AM), <https://news.vice.com/article/online-dating->

fostered an online environment permeated with risks of meeting the wrong person, at the wrong time, in the wrong place.<sup>115</sup> Digital age offenders exploit the “arm-chair approach” to dating which encourages users to feel more comfortable talking to strangers online, without leaving home.<sup>116</sup> When users become comfortable, they assume that they are free to propel the relationship forward by being open and emotionally honest with a stranger, perhaps by sending flirty or sexually explicit messages, and inviting the stranger to the user’s home.<sup>117</sup> As a result, users of mobile dating apps have increased expectations of sexual activity upon the first fact-to-face meeting because they have already established a rapport with the other user, frequently based on openness to and a promise of sex.<sup>118</sup> The excitement of sex and love fuels this perilous environment and leaves users vulnerable to being victimized by unscrupulous users waiting for his or her chance to pounce.<sup>119</sup>

#### B. Crimes of Sexual Violence and Assault

The most frequently reported crimes associated with dating apps are rape, stalking, and the grooming and sexual exploitation of children.<sup>120</sup> Sadly, reports of rape attributed to the use of mobile dating apps have increased 450% in just five years.<sup>121</sup> Offenders persuade and coerce their victims into agreeing to meet early on in the relationship, and are persistent if initially they do not succeed at obtaining sex.<sup>122</sup> The anonymity of the apps makes it easier for offenders to become serial rapists at the tap of a button.<sup>123</sup> This ease is aided by potential victims not thinking of the offender as a stranger, but rather someone he or she has gotten to know.<sup>124</sup>

For example, police in Fremont, California arrested a twenty-year old student who used Tinder to lure at least four unsuspecting victims into meeting him before he sedated and sexually assaulted them.<sup>125</sup> Authorities refer to this assailant

---

rape-reports-rise-450-percent-in-five-years.

<sup>115</sup> *Id.*

<sup>116</sup> *Id.*

<sup>117</sup> *Id.*

<sup>118</sup> *Id.*

<sup>119</sup> *Id.*

<sup>120</sup> Connolly, *supra* note 112.

<sup>121</sup> Wells, *supra* note 114.

<sup>122</sup> *Id.*

<sup>123</sup> *Id.*

<sup>124</sup> *Id.*

<sup>125</sup> Alan Wang, *East Bay Man Allegedly Used Dating Apps to Lure, Rape Women*, ABC7 NEWS (Oct. 5, 2015), <http://abc7news.com/news/east-bay-man-allegedly-used-dating-apps-to-lure-rape-women/1019063/>.

and others as “serial social media rapists.”<sup>126</sup> Users of this kind hide behind their digital profiles and develop trust with their victims before becoming dangerous in the real world.<sup>127</sup> Two other international examples are even more troubling. In New Zealand, a male perpetrator drugged and raped a twenty-eight year old woman with whom he had been communicating on Tinder.<sup>128</sup> Separately in New Zealand, a twenty-six year old woman’s fears of a man’s sexual advances manifested when she jumped off the balcony of a fourteenth-floor apartment – feeling like she had no other option but to engage in sexual intercourse.<sup>129</sup> These examples merely highlight a few of the millions of heinous, sexual assaults that evolve from the use of mobile dating apps every day.<sup>130</sup>

### C. Stalking and Harassment

Although not inherently sexual in nature, stalking<sup>131</sup> is another activity that deceptive users typically exploit through their mobile dating app use.<sup>132</sup> The simple process of sharing the user’s location is commonplace on dating apps, but begs the question whether it should be.<sup>133</sup> Tales of unsuspecting women sharing their locations on dating apps simply to see who else is nearby have culminated in tragedy.<sup>134</sup> Victims of stalking on dating apps have sensed they may be sharing too much personal information on the apps.<sup>135</sup> When confronted with this unsettling feeling, users have the option to block threatening users of the app, but frequently, if this option is pursued, the user may become instigated – forcing

---

<sup>126</sup> *Id.*

<sup>127</sup> *Id.*

<sup>128</sup> Susannah Guthrie, *Rape, Murder and Stalkers: The Real Risks of Tinder*, NEW DAILY (Oct. 9, 2014, 6:58 PM), <http://thenewdaily.com.au/life/relationships/2014/10/09/tinder-app-risks/>.

<sup>129</sup> *Id.*

<sup>130</sup> *See id.* (“There are a number of sexual predators out there who use modern technology to find potential victims.”).

<sup>131</sup> *See generally Stalking*, NAT’L INST. OF JUSTICE, <https://www.nij.gov/topics/crime/stalking/pages/welcome.aspx>. (last visited Dec. 19, 2017) (explaining that the exact definition of stalking varies by state. However, stalking can be conservatively defined as “a course of conduct directed at a specific person that involves repeated (two or more) occasions, with visual or physical proximity, nonconsensual communication, or verbal, written, or implied threats, or a combination thereof, that would cause a reasonable person fear.”).

<sup>132</sup> *See* Henning Wiechers, *Test Report: How Dangerous Is Tinder Stalking*, PR NEWSWIRE (Apr. 21, 2015), <http://www.prnewswire.com/news-releases/test-report-how-dangerous-is-tinder-stalking-500800901.html> (“Dating apps like Tinder are not only a highly frequented address for the quick flirt, but they also offer a welcoming platform for stalkers and snoopers.”).

<sup>133</sup> Lydia Brown, *I Was Stalked by Someone I Met on Tinder*, TAB, <http://thetab.com/uk/york/2016/05/12/i-stalked-someone-i-met-tinder-10249> (last visited Dec. 19, 2017).

<sup>134</sup> *Id.*

<sup>135</sup> *Id.*

the offender to find alternative avenues of contacting the victim.<sup>136</sup>

For instance, once the victim blocks the offender on Tinder, stalkers often find the victim on Facebook and initiate a renewed attempt to communicate with him or her through Facebook Messenger.<sup>137</sup> Even if the victim does not respond to messages, Facebook creates unfettered access to the user's life through tagged photos or posts from users outside the victim-assailant relationship such as mutual friends or friends of only one of the parties.<sup>138</sup> Such posts exhibit geolocation data and allow the assailant to gain information about places the victim frequents.<sup>139</sup> Mobile dating apps have also been known to share the geolocation of its users for up to one hundred and sixty-five days after the initial location share, even if the user has not been using the app, helping facilitate stalking behavior.<sup>140</sup> Based on this information, perpetrators often follow their victims into nightclubs, or other social meeting places, and then home.<sup>141</sup> Access to a plethora of information renders it unsurprising that non-physical crimes, for example the ones perpetrated in cyberspace, are equally as likely to occur through use of mobile dating apps.<sup>142</sup>

#### D. Cyber Crimes

Crimes resembling identity theft and the number of users of mobile dating apps have increased correlatively.<sup>143</sup> Similarly to how perpetrators of violent crimes take advantage of the anonymous yet interpersonal characteristics of the app, perpetrators of non-violent cybercrimes thrive on the victim's desire and willingness for a relationship.<sup>144</sup> They use this vulnerability to coax victims into a relationship of trust before cheating people of their hard earned money.<sup>145</sup> One way users do so is by creating fake profiles within Tinder that are capable of sending messages to various users, tempting them to download mobile games with alluring names, like, "Castle Clash," but for a price.<sup>146</sup> Users then download

---

<sup>136</sup> *Id.*

<sup>137</sup> *Id.*

<sup>138</sup> *Id.*

<sup>139</sup> *Id.*

<sup>140</sup> Guthrie, *supra* note 128.

<sup>141</sup> Brown, *supra* note 133.

<sup>142</sup> *Hook, Line and Tinder: Scammers Love Dating Apps*, NBC NEWS (Apr. 11, 2014, 5:36 PM), <http://www.nbcnews.com/tech/security/hook-line-tinder-scammers-love-dating-apps-n77256>.

<sup>143</sup> *Id.*

<sup>144</sup> *Id.*

<sup>145</sup> *See id.* (detailing how two Colorado residents were arrested for allegedly being responsible for depriving almost 400 people out of \$1 million and explaining that their co-conspiring collaborators around the world are never caught).

<sup>146</sup> *Id.*; Guthrie, *supra* note 128. *See also Castle Clash Wiki*, FANDOM, <http://castle->

these games and effectively enable hackers to access that user's private and personal information.<sup>147</sup> Mal-intentioned users can then create fake profiles by compiling photos and publicly available information posted on any individual's Facebook account and then arranging it to match a believable Tinder profile.<sup>148</sup> This method uses technology built into the app, and users, ensnared by the appealingly authentic profiles, jeopardize the security of their bank accounts with a mere swipe to the right.<sup>149</sup>

Additionally, apps frequently launch automated "scripts"<sup>150</sup> that are systems used to automate responses seemingly from a real person into messages between human users and fake accounts called "bots."<sup>151</sup> Bots are programmed to ask and answer questions with pre-generated and synthetic responses, simulating conversations with real people.<sup>152</sup> Frequently, bots adopt the persona of a soldier in the military stationed overseas who needs money to fly home so the two can meet in person.<sup>153</sup> The sensitive and heroic appeal of this ploy can be emotionally and financially devastating.<sup>154</sup> Once dangerous users obtain private information like email addresses, pictures, and other information over the app, the information is at risk of being hacked by mal-intentioned users.<sup>155</sup> Innocent users are urged to be aware of the financial vulnerabilities as well as the physical pitfalls one might encounter using mobile dating apps.<sup>156</sup> It is crucial for a user to be aware of the types of information that can be retrieved from the mobile dating app if and when the user indeed stumbles into danger from using one of these apps.

---

[clash.wikia.com/wiki/Castle\\_Clash\\_Wiki](http://clash.wikia.com/wiki/Castle_Clash_Wiki). (last visited Dec. 19, 2017) (explaining "Castle Clash is a game where users can create their own fortresses in order to battle other users on the site).

<sup>147</sup> *Hook, Line and Tinder: Scammers Love Dating Apps*, *supra* note 142.

<sup>148</sup> *Id.*

<sup>149</sup> *Id.*

<sup>150</sup> *See generally Script*, TECHTERMS, <https://techterms.com/definition/script> (last visited Dec. 16, 2017) ("A computer script is a list of commands that are executed by a certain program or scripting engine. Scripts may be used to automate processes on a local computer or to generate Web pages on the web.").

<sup>151</sup> *Hook, Line and Tinder: Scammers Love Dating Apps*, *supra* note 142.

<sup>152</sup> *Id.*

<sup>153</sup> *Id.*

<sup>154</sup> *Id.*

<sup>155</sup> Simon Edmunds, *Personal Data at Risk on Apps Like Tinder and Grindr Says Research*, GLOBAL DATING INSIGHTS (May 20, 2015), <http://globaldatinginsights.com/2015/05/20/20052014-personal-data-at-risk-on-apps-like-tinder-and-grindr-says-security-research/> (citing Jody Farnden, Ben Martini & Kim-Kwang Raymond Choo, *Privacy Risks in Mobile Dating Apps 2* (2015) Proceedings of the 21st Americas Conference on Information Systems, Conference in Puerto Rico 13-15, <https://arxiv.org/pdf/1505.02906.pdf>).

<sup>156</sup> *Id.*



## INFORMATION STORED AND RETRIEVABLE FROM MOBILE DATING APPS

## A. Geolocation Data

As highlighted above, mobile dating apps would cease to exist if it were not for geolocation or Location Based Services.<sup>157</sup> Geolocation records tend to show users' exact location by using latitude and longitude coordinates.<sup>158</sup> It is alarming to note that basically all of these statistics are compiled and stored on the app itself. For example, Grindr users' locations are sent from personal cellphones to the app server.<sup>159</sup> From there, country and city data, determined by latitude and longitude coordinates, is recorded and stored within the server.<sup>160</sup> Moreover, the Grindr app stores timeframes of all of the user's activity. For example, the app stores timeframes when messages are sent and received, as well as where the user is located at the time of sending and receiving those messages.<sup>161</sup> Tinder shares similar timeframes based on where the user is located when he or she opens the app using latitude and longitude coordinates.<sup>162</sup> Taken together, these components "can be used to track users that stay connected to the same network."<sup>163</sup> As a result, geolocation records of a specific user could be used to recreate the timeline associated with the perpetration of a crime.<sup>164</sup> By permitting officers to inspect the phone of an alleged assailant, officers are able to obtain a more complete representation of not only the timeline of the crime, but also to take a look into the comprehensive nature of the relationship between the victim and the perpetrator in the moments leading up to the commission of the crime.<sup>165</sup>

## B. Private Information

Unfortunately, most users are unaware of all the personal information they offer to the public through their mobile dating apps.<sup>166</sup> Recent studies have analyzed the data that is recoverable from mobile dating apps, including Tinder and

---

<sup>157</sup> *Always Be Oriented with the Integration of Geolocation into Your App*, *supra* note 51.

<sup>158</sup> *Geolocation – FAQs*, APNIC, <https://www.apnic.net/get-ip/faqs/geolocation/> (last visited Dec. 19, 2017).

<sup>159</sup> Farnden, *supra* note 17, at 2, 6.

<sup>160</sup> *Id.* at 5-6.

<sup>161</sup> *Id.* at 2, 8.

<sup>162</sup> *Id.* at 6.

<sup>163</sup> *Id.*

<sup>164</sup> *Id.* at 2, 10.

<sup>165</sup> *Id.* at 2.

<sup>166</sup> *Id.* at 9.

Grindr, once the mobile phone is in the hands of law enforcement, or worse, a criminal.<sup>167</sup> A breakdown of the technological makeup of the apps themselves, including the study of functional command paths,<sup>168</sup> is used in deciphering what information is stored within the app.<sup>169</sup> Aside from revealing email addresses, pictures, and private text and chat messages, if desired, officials or hackers can access images of all nearby dating app user accounts with which a specific user recently has interacted.<sup>170</sup> If he or she is using Tinder, accessible data can include “matches” with innocent users, as well as the dates the “matches” occurred.<sup>171</sup> Analyzing “matches” allows an interested party to establish the connection between user accounts.<sup>172</sup> Law enforcement can use this association as a starting point for investigations of crimes related to mobile dating app use.<sup>173</sup> Once “matches” are known, message tables<sup>174</sup> housed within the app reveal messages sent and received by the user with timestamps, for each.<sup>175</sup> Grindr stores the same types of information as well as account information for other profiles linked to the user’s account like Instagram, Twitter, or Facebook.<sup>176</sup> The feasibility of extracting private information paired with geolocation data from mobile dating apps creates the possibility of reconstructing crimes to prosecute perpetrators of offenses.<sup>177</sup>

#### LEGAL IMPLICATIONS OF ACCESSING INFORMATION STORED ON THE APPS

There is a vast difference between privacy risks associated with obtaining geolocation data from an app on a cellphone and private information such as messages, stored within a cellphone.<sup>178</sup> Cellphones and apps are “constantly generating and sending a wealth of information to cell service providers who, in turn,

---

<sup>167</sup> *Id.* at 2.

<sup>168</sup> *See generally* *What are PATH and other environment variable, and how can I set or use them?*, SUPERUSER, <https://superuser.com/questions/284342/what-are-path-and-other-environment-variables-and-how-can-i-set-or-use-them>. (last visited Dec. 19, 2017) (explaining that functional command paths are codes designed to specify paths or command lines to different programs indicating a function to perform).

<sup>169</sup> Farnden, *supra* note 17, at 2-3.

<sup>170</sup> *Id.* at 2; Edmunds, *supra* note 155.

<sup>171</sup> *See generally* Farnden, *supra* note 17, at 8, 14-15.

<sup>172</sup> *Id.* at 7-8, 14-15.

<sup>173</sup> *See generally id.*

<sup>174</sup> *See generally id.* (illustrating that message tables, a direct snapchat of a string of messages, contain descriptive information including the user ID of the chat partner, the ID of the match between the user and the chat partner, the timestamp of the message, if there is an error in sending the message, the body of the message, and if the message has been read).

<sup>175</sup> *Id.* at 8.

<sup>176</sup> *Id.* at 5-6.

<sup>177</sup> *See generally id.* at 1-2.

<sup>178</sup> *See generally* Lauren E. Babst, *No More Shortcuts: Protect Cell Site Location Data*

store [the] information.” This information, including personal information and geolocation data stored within mobile dating apps, is retrievable from the phone.<sup>179</sup> The pervasiveness of cellphones in today’s society presents new concerns for courts forced to decide whether the Fourth Amendment protections should apply to all or some of the various types of data stored in cellphones.<sup>180</sup> As a result, the scope of the Fourth Amendment and geolocation data is distinguishable from the private information stored on a cellphone and individual apps.<sup>181</sup> The purview of the Fourth Amendment must be analyzed and applied to private information separately from geolocation data gathered from mobile dating apps.<sup>182</sup> The privacy risks attributable to either type of data directly limits the items that can lawfully be searched under the Fourth Amendment with either a warrant or a subpoena.<sup>183</sup> The text of the Fourth Amendment guarantees:

The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.<sup>184</sup>

Thus, the Supreme Court in *Katz v. United States* articulated that the government conducts a search within the meaning of the Fourth Amendment when it violates an individual’s reasonable expectation of privacy in property worthy of a “subjective expectation of privacy . . . that society is prepared to recognize [that expectation of privacy] as ‘reasonable.’”<sup>185</sup> Therefore, the Fourth Amendment’s

---

*with a Warrant Requirement*, 21 MICH. TELECOMM. & TECH. L. REV. 363, 373-375, 377 (2015) (discussing how CSLI (Cell-Site Location Information) can be used to track individual’s locations and communications, and when it can become a violation of an individual’s right to privacy under the Fourth Amendment).

<sup>179</sup> *Id.* at 371-72.

<sup>180</sup> *See id.* at 364 (“The pervasiveness of cellphones in modern society has presented new concerns for individuals’ privacy and forced courts to decide whether Fourth Amendment protections should apply to the data that cellphones generate”). *See also* *United States v. Graham*, 846 F. Supp. 2d 384, 388 (4th Cir. 2012); *In re United States of America for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers*, 416 F. Supp. 2d 390, 397 (4th Cir. 2006) (holding probable cause is the appropriate standard for government access to prospective cell site location data without a warrant).

<sup>181</sup> *See* Babst, *supra* note 178, at 364-66 (explaining that until recently, courts were using cases from the 1970’s and 1980’s, which only address primitive aspects of today’s technology, but now government access to geolocation data has opened a door to further access). *See generally* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 681-83 (2011).

<sup>182</sup> Babst, *supra* note 178, at 369.

<sup>183</sup> *Id.* at 365-70.

<sup>184</sup> U.S. CONST. amend. IV.

<sup>185</sup> *See Katz v. United States*, 389 U.S. 347, 353, 360-61 (1967) (Harlan, J., concurring)

powers ought to protect an individual's reasonable expectation of privacy of technological progressions outside the purview of the Framers' intentions.<sup>186</sup> Although it is a basic principle of the Fourth Amendment that searches and seizures of anything in general without a warrant are "presumptively unreasonable," or unfounded in the law, there are a few exceptions, and geolocation data attainable from cellphones and apps is one of those exceptions.<sup>187</sup>

#### A. Obtaining Geolocation Data

Cell phone users, more specifically mobile dating app hopefuls, have a lower expectation of privacy in their geolocation data in comparison to other intimate information stored within their phones.<sup>188</sup> Apps that rely on geolocation technology, like mobile dating apps prompt the user for permission to access his or her location; even if the user denies access once, the request for permission will reappear upon reopening the app or upon turning on the phone.<sup>189</sup> By granting the dating app permission, users are essentially re-acknowledging their acceptance to the Terms and Conditions of that app to which they agreed when they signed up.<sup>190</sup> This standard agreement typically includes provisions expressing the no-

---

(articulating precedent which established this twofold requirement and explaining that although a man's home is protected, objects exposed to the "plainview of outsiders" are not protected because there was no intention to keep them private, including "conversations in the open"). *See also* *Kyllo v. United States*, 533 U.S. 27, 32-33 (2001). *See generally* *United States v. Karo*, 468 U.S. 705, 712-13 (1984) (holding that no Fourth Amendment interest is infringed by the installation of a beeper, but the monitoring thereof may impair the individual's privacy).

<sup>186</sup> Babst, *supra* note 178, at 377; *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 143 (E.D.N.Y. 2013). *See also* *United States v. Jones*, 565 U.S. 400, 403-10 (2012) (distinguishing between warrantless installations of location monitoring via a tracking device from situations involving electronic signals). Monitoring via tracking device does not involve a physical trespass and ought to be analyzed under the *Katz* framework. *In re Smartphone Geolocation*, 977 F. Supp. 2d at 138. *See also* *Katz*, 389 U.S. at 360-61 (defining a two-pronged approach to defining "reasonable expectation of privacy." The twofold requirement is that the person must have exhibited an actual (subjective) expectation of privacy and, that the expectation be one that society is prepared to recognize as reasonable).

<sup>187</sup> Babst, *supra* note 178, at 377-79.

<sup>188</sup> *See generally In re Smartphone Geolocation*, 977 F. Supp. 2d at 137-38 (describing why cell phone users choosing not to turn off their location settings due to interference with the proper functioning of popular apps such as parental controls, GPS, weather predictions and social media).

<sup>189</sup> *Id.* at 138.

<sup>190</sup> *Id.* (explaining that by smartphone users receiving frequent notifications and reminders of location service settings, they are essentially re-acknowledging their consent to the Terms and Conditions of the app in question).

tion that information such as geolocation may be stored within the app and provided or disclosed, if required to do so by law.<sup>191</sup> However, to avoid the continuous transcription of geolocation data, users of Smartphones and apps are also inherently aware of the readily accessible fact that turning off one's phone, or turning off geolocation services on an individual app, ceases those communications between the phone and third parties, including service providers.<sup>192</sup> Yet, by keeping the phone powered on and by accessing mobile dating apps, users are aware of the dangers and thus assume the risk that the information will continuously be recorded and possibly sent to third parties.<sup>193</sup>

Not only are users cognizant this information is stored by the provider and therefore can be handed over to others, they expressly agree to these terms through the provider's standard Terms and Conditions.<sup>194</sup> A central element in determining whether an individual has a reasonable expectation of privacy in certain data is the effort made to keep the subject information private.<sup>195</sup> Thus, by willingly and actively transmitting this information to others, users' expectation of privacy in their geolocation data is unreasonable.<sup>196</sup> Therefore, the Fourth Amendment does not extend to the geolocation data on cellphones and mobile dating apps, and retrieving this information would not be a search afforded constitutional protections.<sup>197</sup> Obtaining geolocation data from a third-party service provider or directly from the apps should merely require a subpoena instead of a warrant because it does not rise to the level of a search under the parameters

---

<sup>191</sup> *Id.* at 139-41. *See also Terms of Use, TINDER*, <https://www.gotinder.com/terms> (last visited Dec. 19, 2017) (indicating that users agree and allow Tinder to access, preserve, and disclose account information/content if required to do so by law).

<sup>192</sup> *In re Smartphone Geolocation*, 977 F. Supp. 2d at 138-39, 141. *See also* Alexander Aciman, *How to Stop Your Phone from Tracking Your Location*, TIME (Feb. 20, 2015), <http://time.com/3716950/location-tracking-turn-off/> (explaining that turning a cell phone's location services off allows a user to avoid detection via geolocation because it prevents the device's internal GPS from tracking the user's whereabouts and subsequently distributing that information to apps).

<sup>193</sup> *In re Smartphone Geolocation*, 977 F. Supp. 2d at 139, 142.

<sup>194</sup> *Id.* at 141-42 (explaining that cell phone service providers may require "users to agree to terms and conditions that include its privacy policy, which governs [the] company's use of personal information. That policy provides that [the cell service] may automatically collect your information when you use your mobile device or [the cell service's] or websites, including: [y]our phone number and device identifier [and] [t]he location of your device on our network and the GPS location of your device.").

<sup>195</sup> *Id.* at 146.

<sup>196</sup> *Id.* at 147. *See generally* United States v. Caraballo, 963 F. Supp. 2d 341, 354, 356 (D. Vt. 2013) ("A Fourth Amendment analysis entirely dependent upon the fortuity of a criminal defendant entering his or her own home during the pinging process is likely to prove as unworkable as the definition of "short term" GPS location monitoring Justice Alito deemed presumptively reasonable.").

<sup>197</sup> *In re Smartphone Geolocation*, 977 F. Supp. 2d at 147.

of *Katz* or of the Fourth Amendment.<sup>198</sup>

### *Subpoenas vs. Warrants*

All three branches of the U.S. government possess what has colloquially been called the “subpoena power.”<sup>199</sup> The power to issue subpoenas refers to “the authority to command persons to appear and testify or to produce documents or things.”<sup>200</sup> A subpoena launches an adversary process during which the person served with the subpoena can challenge its demand in court before complying with the order.<sup>201</sup> Despite the option to challenge, this strong federal power has thrust itself into the government’s responsibilities of investigation and inquisition.<sup>202</sup> The government can open investigations through issuing a subpoena merely “on suspicion that the law is being violated, or even just because it wants assurance that it [was] not.”<sup>203</sup> This ability is because of the adversary process inherent in a subpoena, requiring the production of documents or other things, but only after the judicial process is fully afforded to the subject.<sup>204</sup> This lower threshold of certainty, compared to probable cause specific to issuance of a warrant, is a result of the less-invasive nature of the types of information retrievable through a subpoena.<sup>205</sup>

As a result, a person served with a subpoena is entitled to the Fourth Amendment’s protection against unreasonableness, but in a different way than a warrant.<sup>206</sup> For example, the Fourth Amendment protects people against “unreasonable searches and seizures” by imposing a stringent probable cause requirement on the warrant due to the potential immediacy and intrusiveness of the search or seizure to be conducted.<sup>207</sup> A warrant’s “reasonableness” under the Fourth Amendment hinges on whether or not the search or seizure itself would be reasonable under the circumstances.<sup>208</sup> On the other hand, the “reasonableness” of a subpoena is determined by whether the act directed by the subpoena, e.g. the production of documents, is reasonable in light of all of the circumstances.<sup>209</sup> A

---

<sup>198</sup> *Id.* at 142.

<sup>199</sup> 2 U.S.C. §§ 190(l)-(m) (2012) (governing Senate subpoenas).

<sup>200</sup> See *In re Subpoena Duces Tecum*, 228 F.3d 341, 346 (2000) (quoting *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (4th Cir. 1950)).

<sup>201</sup> *Id.* at 346.

<sup>202</sup> *Id.* (citing *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950)).

<sup>203</sup> *Id.* at 347 (quoting *United States v. Morton Salt Co.*, 338 U.S. 632, 643 (1950)).

<sup>204</sup> *Id.* at 346-47.

<sup>205</sup> *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 136-37 (E.D.N.Y. 2013).

<sup>206</sup> *In re Subpoena Duces Tecum*, 228 F.3d at 346-349 (citing *Hale v. Henkel*, 201 U.S. 43, 76 (1906)) (emphasis in original).

<sup>207</sup> U.S. CONST. amend. IV; *In re Subpoena Duces Tecum*, 228 F.3d at 347.

<sup>208</sup> *In re Subpoena Duces Tecum*, 228 F.3d at 347.

<sup>209</sup> *Id.* at 348.

person in receipt of a subpoena can choose to comply with its terms or face contempt charges; while a person's property that is the subject of a warrant has no choice but to be searched or seized.<sup>210</sup> As such, the Fourth Amendment imposes the higher standard of probable cause only to warrants because of the intrusive nature of the conduct inherent in carrying out a search or seizure warrant, contradictory to the say of the individual.<sup>211</sup> A probable cause standard for warrants is necessary to protect against the risk of invading an individual's privacy in personal property to which he or she has demonstrated a reasonable expectation of privacy.<sup>212</sup>

A subpoena should not be issued unless there is a showing that the information from the geolocation record of the user's phone will help apprehend or convict a suspect to a crime related to mobile dating apps.<sup>213</sup> In *In re Smartphone Geolocation Data Application*, the Court in this instance found geolocation records helped apprehend or convict the suspect because undercover officers had been able to contact the suspect on that specific phone two times over the past several days.<sup>214</sup> Additionally, the Court held that for the future, one can obtain geolocation data, with only a subpoena, based on a showing of how it would help apprehend or convict a suspect.<sup>215</sup> The Court's reasoning was based on the fact that the subpoena would only reveal a record of the user's location and nothing further.<sup>216</sup> Since the user's location is freely offered to third parties the relatively low expectation of privacy in this information necessitates only a court-ordered subpoena instead of a warrant.<sup>217</sup>

In the specific instance of *In re Smartphone Geolocation Data Application*, the government had sufficient cause to seek not only prospective geolocation data for the defendant's cellphone for the past 30 days, but it also granted an order directing the third-party cellphone carrier, to "initiate a signal to determine the location of the subject telephone...unobtrusively," to apprehend the defendant at his location.<sup>218</sup> Since the individual had no legitimate expectation of privacy in the location of his cellphone, the government's actions were valid.<sup>219</sup> If the defendant wished not to be located by his cell phone, he should have powered

---

<sup>210</sup> *Id.*

<sup>211</sup> U.S. CONST. amend. IV; *In re Subpoena Duces Tecum*, 228 F.3d at 348.

<sup>212</sup> U.S. CONST. amend. IV; *In re Subpoena Duces Tecum*, 228 F.3d at 348.

<sup>213</sup> *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 137 (E.D.N.Y. 2013).

<sup>214</sup> *Id.* at 133, 150.

<sup>215</sup> *Id.* at 150.

<sup>216</sup> *Id.* at 142.

<sup>217</sup> *Id.* at 142.

<sup>218</sup> *Id.* at 132-33.

<sup>219</sup> *Id.* at 131.

it off.<sup>220</sup>

If law enforcement were to conduct similar practices on the cellphones of suspected perpetrators of crimes on mobile dating apps, they would be able to swiftly apprehend offenders.<sup>221</sup> Prosecutors can access geolocation of both victims and defendants to match timelines, identify shared locations between the victim and the suspect, and identify the assailant with specific, articulable facts, to show that the records are relevant to the criminal investigation.<sup>222</sup> Fortunately for the prosecution, the legal threshold for issuing a subpoena is low in comparison to that for a warrant.<sup>223</sup> The information contained within geolocation records can aid in the prosecution of suspects involved with crimes on mobile dating apps and can be attained easily.<sup>224</sup>

#### *The Electronic Communications Privacy Act*

Although the Fourth Amendment does not extend to geolocation data, this information is nevertheless somewhat protected under the law.<sup>225</sup> The disclosure of geolocation data through a subpoena is governed under the procedures established in the Electronic Communications Privacy Act (“ECPA”).<sup>226</sup> The relevant part of the ECPA provides as follows:

A governmental entity may require a provider of electronic communication service or remote computing device to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the government entity

(A) Obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure...; [or]

(B) Obtains a court order for such disclosure under subsection (d) of this section.<sup>227</sup>

Under subsection (B), the government, with a lesser threshold than probable cause, must present “specific and articulable facts showing there are reasonable grounds to believe the contents of . . . records of other information sought are

<sup>220</sup> *Id.*

<sup>221</sup> Farnden, *supra* note 17, at 2 (showing extent of private information that is collected by dating apps and how law enforcement can use information to catch criminal offenders).

<sup>222</sup> *Id.* at 10.

<sup>223</sup> See *United States v. Morton Salt Co.*, 70 S.Ct. 357, 363-64 (1950) (noting that an administrative agency may investigate based on suspicion that a law is being violated); U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 128 (2009), <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>.

<sup>224</sup> See generally Farnden, *supra* note 17, at 2 (showing types of private information that can be obtained through dating apps).

<sup>225</sup> *In re Smartphone Geolocation*, 977 F. Supp. 2d at 147.

<sup>226</sup> *Id.*

<sup>227</sup> 18 U.S.C. § 2703(c) (2012); *In re Smartphone Geolocation*, 977 F. Supp. 2d at 148.



relevant to an ongoing criminal investigation.”<sup>228</sup> Although the ECPA appears to say that the government can only obtain geolocation data through a search warrant or court order, under § 2703(d), Congress purposefully excluded “any communication from a tracking device” in its definition of “electronic communication.”<sup>229</sup> In the ECPA, “mobile tracking device” is defined as “an electronic or mechanical device which permits the tracking of the movement of a person or object.”<sup>230</sup> Courts have been reluctant to construe “tracking device” to mean a cellphone.<sup>231</sup> For instance, the court in *In re Smartphone Geolocation Data* provided that something as simple as a bicyclist leaving tire tracks in a muddy path would constitute an “electronic or mechanical device which permits the tracking of the movement of a person or object” under the ECPA.<sup>232</sup>

The ECPA is aimed at devices designed solely to track someone or something, such as GPS, as opposed to cellphones, which incidental to their imagined purpose, can be tracked.<sup>233</sup> Therefore, rendering a cellphone subject to this definition is inconsistent with the statute because they were not designed for the purpose of tracking.<sup>234</sup> The government may viably seek a court order or a subpoena for geolocation data under § 2703(d), if supported by “specific and articulable facts” that the records are material to a criminal investigation.<sup>235</sup> However, such a comparatively low threshold for the issuance of a court order or subpoena to obtain geolocation records differs significantly compared to the probable cause required to search private information within mobile dating apps such as messages and contacts.<sup>236</sup>

### B. Obtaining Private Information

The scope of the Fourth Amendment, although failing to reach geolocation data, pierces the private information stored within cellphones and mobile dating apps.<sup>237</sup> Users have a heightened expectation of privacy in the content of the in-

---

<sup>228</sup> 18 U.S.C. § 2703(d) (2012); *In re Smartphone Geolocation*, 977 F. Supp. 2d at 148.

<sup>229</sup> 18 U.S.C. § 3117 (1986); *In re Smartphone Geolocation*, 977 F. Supp. 2d at 148.

<sup>230</sup> 18 U.S.C. § 3117 (1986); *In re Smartphone Geolocation*, 977 F. Supp. 2d at 148.

<sup>231</sup> *In re Smartphone Geolocation*, 977 F. Supp. 2d at 150.

<sup>232</sup> *Id.* (citing 18 U.S.C. § 3117(b) (2012)).

<sup>233</sup> *Id.*

<sup>234</sup> *Id.*

<sup>235</sup> *Id.* at 148 (citing 18 U.S.C. § 2703(d) (2012)).

<sup>236</sup> *Id.*; *In re Cellular Tels.*, No. 14-MJ-8017-DJW, 2014 WL 7793690, at \*1, 3 (D. Kan. Dec. 30, 2014).

<sup>237</sup> *See Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (discussing mobile dating application’s range of tools for managing information).

formation stored on his or her cellphone in comparison to geolocation data emitted from the cellphone.<sup>238</sup> Therefore, if the collection of this private information were to be searched, it would be awarded the protections of a search under the Fourth Amendment.<sup>239</sup> To obtain information stored within a standard Smartphone, the government or operating law enforcement capacity must therefore obtain a search warrant under the protections of the Fourth Amendment before searching the phone for private information known to be stored within various apps.<sup>240</sup> If the warrant is not stated with enough particularity, courts have been known to reject applications for search warrants, even if supported by probable cause that the information to be searched will aid in an apprehension or conviction.<sup>241</sup>

### *The Particularity Requirement of a Warrant*

Applying Fourth Amendment constitutional protections in the modern digital age has proved difficult.<sup>242</sup> Enhanced technology now allows an individual to carry personal information, including potential love interests, around in the palm of his or her hand. However, fingertip accessibility does not render such personal information any less worthy of the protections guaranteed under the Constitution.<sup>243</sup> This raises an interesting concern of what exactly can be searched within a cellphone's wealth of information. Therefore, the particularity requirement necessitated by the Fourth Amendment plays an increasingly important role in today's society.<sup>244</sup>

In issuing a search warrant for private information stored within a mobile dating app, the court must balance the interests of an individual's right to privacy and the government's ability to prosecute suspects of crimes on mobile dating apps efficiently and effectively.<sup>245</sup> One way of ensuring that this balance is maintained is by requiring that warrants contain precise and particular limits on the scope of the proposed search.<sup>246</sup> Since cellphones and Smartphones have evolved to hold vast amounts of "the privacies of life" including sensitive information akin to cameras, video players, rolodexes, calendars, libraries, diaries, and maps,

---

<sup>238</sup> *Id.* at 2489.

<sup>239</sup> *Id.*; *Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring) (explaining the expectation of privacy individuals and the public must have for protection).

<sup>240</sup> *Riley*, 134 S. Ct. at 2488-89; Farnden, *supra* note 17, at 12-1.

<sup>241</sup> *In re Cellular Tels.*, 2014 WL 7793690, at \*7.

<sup>242</sup> *In re Cellular Tels.*, 2014 WL 7793690, at \*3.

<sup>243</sup> *See Riley*, 134 S. Ct. at 2488-90 (describing heightened expectations of privacy due to the volume of personal information typically contained in a modern arrestee's cellphone).

<sup>244</sup> *In re Cellular Tels.*, 2014 WL 7793690, at \*5.

<sup>245</sup> *Id.* at \*3.

<sup>246</sup> *Id.* at \*3-4.

the boundaries described within the application for a search warrant must contain clear parameters of the exact app or function of the phone that is to be searched.<sup>247</sup>

The only feasible way to describe “the place to be searched” within a Smartphone or app, is to specify how to search each app, as opposed to simply permitting their search generally.<sup>248</sup> For example, applications for search warrants pertaining to mobile dating apps should contain a search protocol explaining how the search will separate what the search is permitted to explore from what is not.<sup>249</sup> The government or law enforcement entity must be as detailed as possible, while using intricate, technical formulations, explaining how to gain access to the types of information stored within the app via commands and queries.<sup>250</sup> This attention to detail illustrates how the government can make focused efforts to limit itself to the particularized scope of the search being sought.<sup>251</sup> If the government is successful in its attention to detail, the court will likely issue the warrant.<sup>252</sup> Thus, private information stored within mobile dating apps like messages, matches, and texts, can be searched in connection with an ongoing criminal investigation associated with relationships formed on mobile dating apps.<sup>253</sup>

## CONCLUSION

Mobile dating apps have presented society with puzzling new obstacles in the 21<sup>st</sup> century.<sup>254</sup> The millions of users who enjoy such apps have adopted a new method of finding love in the digital age at the touch of a button.<sup>255</sup> Unfortunately, the hopeful optimism and convenience of sharing in-depth, personal information online with strangers can put the user’s safety and well-being in jeopardy. If a crime is committed, as a recourse, information can be extracted and used against a fellow user of a mobile dating app. A mal-intentioned user’s geolocation data can be obtained with a subpoena or court order, which requires a

---

<sup>247</sup> *Id.*

<sup>248</sup> *Id.* at \*8.

<sup>249</sup> *Id.*

<sup>250</sup> *Id.*

<sup>251</sup> *Id.*

<sup>252</sup> *Id.* at \*8-9.

<sup>253</sup> *Id.* at \*3-4; Farnden, *supra* note 17, at 12.

<sup>254</sup> Anthony Wing Kosner, *Tinder Dating App Users Are Playing with Privacy Fire*, FORBES (Feb. 18, 2014, 11:20 AM), <https://www.forbes.com/sites/anthonykosner/2014/02/18/tinder-dating-app-users-are-playing-with-privacy-fire/#41a2ab8d3dbd>.

<sup>255</sup> See Sophia Kercher, *First Comes Tinder. Then Comes Marriage?*, N.Y. TIMES, Apr. 19, 2017, at D5 (suggesting that many tinder users are seeking committed relationships and finding long-term love partners by using the app).

lesser evidentiary threshold than a warrant supported by probable cause. Probable cause is not required because the user lacks a reasonable expectation of privacy in his or her geolocation and such data can be obtained without a warrant.

In comparison, users have a sufficient reasonable expectation of privacy in their private information data under the scope of the Fourth Amendment. This reasonable expectation of privacy requires a warrant pointing to specific, articulable facts that explain how such data will inevitably lead to the conviction or apprehension of a suspect in a crime relating to a relationship formed on a mobile dating app. A warrant will be issued if the government, whether it be law enforcement or the prosecutor, can indicate with articulable facts that such information will assist in the conviction or apprehension of a suspect of a crime known to be associated with mobile dating apps. An application for a warrant pertaining to the search of a cellphone must state with particularity the data within the phone to be searched. If issued, the warrant will uphold the balance between privacy risks and the protection of private information, so that justice might be achieved in catching perpetrators of crimes on mobile dating apps.