DISTRICT COURT, ARAPAHOE COUNTY, STATE OF COLORADO 7325 S. Potomac St. Centennial, Colorado 80112	▲COURT USE ONLY▲
PEOPLE OF THE STATE OF COLORADO **v.** **JAMES EAGAN HOLMES,** **Defendant**	Case No. **12CR1522** Division: **201**
ORDER REGARDING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE: RECORDS OBTAINED FROM MATCH.COM AND ADULT FRIEND FINDER (D-117)	

INTRODUCTION

In this Order, the Court addresses the defendant's motion to suppress records obtained by law enforcement from two internet dating websites, AdultFriendFinder.com and Match.com.[1] The prosecution opposes the motion. The Court held a non-evidentiary hearing on October 7 and October 10, 2013.

For the reasons articulated in this Order, the motion is denied. Part of the motion is moot because the prosecution does not intend to introduce into evidence

[1] "Adult Friend Finder" is described by Wikipedia as "an online sex and swinger personals community website" that "allows members to meet new friends or sex partners." *See* Response, Ex. 2 at pp. 7-8; *see also* http://en.wikipedia.org/wiki/Adult_FriendFinder. The site "claims to have over 30 million members." http://en.wikipedia.org/wiki/Adult_FriendFinder. Match.com describes itself as "an online dating" service and claims to serve "millions of singles in 24 countries." *See* http://www.match.com.

records containing any communications between the defendant and other members of the websites. The rest of the motion fails because the defendant did not meet his burden of demonstrating a constitutionally protected expectation of privacy in the profile records and subscription records. Accordingly, law enforcement did not need an order or a warrant to obtain those records.

BACKGROUND

The defendant is charged with shooting, and killing or injuring, numerous people inside two adjacent Aurora movie theatres at approximately 12:30 a.m. on July 20, 2012. On July 21, 2012, TMZ reported that "[a] man claiming to be James Holmes" had created a profile on AdultFriendFinder.com on July 5, 2012, which "included a picture of himself with reddish, orange hair . . . just as officials in Aurora, CO said he looked when he was apprehended . . . ." *See* James Holmes – Cops Investigating Sex Site Profile, TMZ.com, http: //www.tmz.com/2012/07/20/james-holmes-sex-website-penis-cops (last visited Nov. 6, 2013).[2] According to the report, "'Holmes'—who used the screen name classicjimbo—included a cryptic message on the top of the profile which read[], 'Will you visit me in prison?'" *Id.*

[2] The photograph on the published profile matches the defendant's physical appearance at the time of his arrest.

The published AdultFriendFinder.com profile contained information about the defendant's height, marital status, and body type. It also disclosed information about whether he drank, smoked, and used drugs.

The following day, TMZ reported that it had learned from a woman named Diana, a member of Match.com, that she had seen the defendant's profile on Match.com just hours after the shooting as one of her matches. *See* Colorado Shooting Suspect James Holmes – The Match.Com Profile, TMZ.com, http://www.tmz.com/2012/07/22/james-holmes-colorado-shooting-match-profile (last visited Nov. 6, 2013). The report stated that "[t]he profile also ha[d] the same tagline from [the defendant's] adultfinder.com profile—'Will you visit me in prison?'" *Id.*

The published Match.com profile included the defendant's photograph, his age, his height, his body type, his ethnicity, his city of residence, and his marital status. It also included information about what types of dates he was seeking, whether he had children, whether he wanted children, his favorite movies, his favorite book, his political views, his faith, whether he smoked, whether he drank, and how he liked to spend his time.

During the hearing, the prosecution specifically referred to the TMZ reports and represented that, upon becoming aware of the reports, law enforcement applied for two separate out-of-state orders for the production of the defendant's records

from Match.com and AdultFriendFinder.com.[3] More specifically, law enforcement applied for: (1) a court order, pursuant to 18 U.S.C. § 2703 (2012), for the defendant's Match.com records from the district court in Dallas County, Texas, where Match.com is apparently headquartered; and (2) a search warrant, pursuant to the California Penal Code, for the defendant's AdultFriendFinder.com records from the superior court in Santa Clara, California, where AdultFriendFinder.com is apparently headquartered. *See* Response, Exs. 1, 2.

ISSUES PRESENTED AND RULINGS

In support of Motion D-117, the defendant raises multiple challenges to the Texas order and the California warrant that authorized law enforcement to obtain records from Match.com and AdultFriendFinder.com. *See generally* Motion and Reply. At the hearing, the defendant clarified that he seeks to exclude three categories of records obtained: (1) his profile records; (2) subscription records the

[3] Attached to the affidavit in support of the request for production of the AdultFriendFinder.com records was an article similar to the two TMZ reports. *See* Response, Ex. 2. This article—titled "James Holmes Alleged Adult Friend Finder Profile And 'The Joker' Photos,"—was posted by The Inquisitr on July 21, 2012, and contained even more information than the TMZ article, including the defendant's "Gold level" AdultFriendFinder.com membership; it also included the same images of the defendant's AdultFriendFinder.com profile that were published by TMZ. *See* Response, Ex. 2. Pursuant to CRE 201(c), the Court, in its discretion, takes judicial notice of the internet postings of these articles, but not of the accuracy of their contents. All three articles are attached to this Order (the TMZ articles are Attachments 1 and 2; the article from The Inquisitr is Attachment 3).

websites had on file for him;[4] and (3) records containing his communications with other members of the websites.

In response, the prosecution informed the Court that it does not intend to introduce the contents of any private messages between the defendant and other members of the websites. The prosecution stated, however, that it does plan to present evidence from the defendant's Match.com and AdultFriendFinder.com profiles and subscription records. The prosecution contends that the defendant lacks standing to challenge the production of these documents because he cannot demonstrate a reasonable expectation of privacy in them. Response at p. 1.

The request to suppress records containing communications between the defendant and other members of Match.com and AdultFriendFinder.com is denied as moot. The remainder of the motion is denied because the Court agrees with the prosecution that the defendant did not demonstrate a constitutionally protected expectation of privacy in his profile records and the records containing subscription information. This determination, in turn, renders addressing the merits of the challenges raised in Motion D-117 unnecessary.

---

[4] At the hearing, the prosecution explained that the following items are included in the subscription records obtained: (1) identifying information, such as the defendant's name, email addresses, billing history, and Internet Protocol ("IP") address; and (2) dates when the accounts were activated and log data, such as times of log in and the duration of sessions. An IP address is a unique identifier that is assigned through an internet service provider. *United States v. Christie*, 624 F.3d 558, 563 (3d Cir. 2010). Each IP address corresponds to an internet user's individual computer. *Id.* When an internet user visits a particular website, the site administrator is able to view the IP address. *Id.* Thus, through the defendant's IP address, each website's administrator was able to collect his log data.

ANALYSIS

The defendant avers that he has a reasonable expectation of privacy in his profiles and the subscriber information he provided or exposed to the administrators of Match.com and AdultFriendFinder.com. Motion at p. 3. Therefore, asserts the defendant, these records are protected by both the Fourth Amendment to the United States Constitution and article II, section 7, of the Colorado Constitution. *Id.* The Court disagrees.

I. Legal Standard Governing Expectation of Privacy Claims

A. United States Constitution

The Fourth Amendment to the United States Constitution prohibits "unreasonable searches and seizures." *Camara v. Mun. Court*, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967). The purpose of this constitutional protection "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Id.*

In *Katz v. United States*, the United States Supreme Court analyzed the scope of the protection afforded by the Fourth Amendment. 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). When an individual challenges governmental investigative activity under the Fourth Amendment, *Katz* requires a two-part inquiry: (1) did the person seeking protection under the Amendment exhibit an actual (subjective) expectation of privacy; and (2) is that expectation one that

society is prepared to recognize as reasonable. *Id.* at 361, 88 S.Ct. 507 (Harlan, J., concurring). Thus, in order to challenge a search or seizure under the Fourth Amendment, an individual must have a subjective expectation of privacy in the place or property to be searched, and that expectation must be objectively reasonable. *Minnesota v. Olson*, 495 U.S. 91, 95-96, 110 S.Ct. 1684, 109 L.Ed.2d 85 (1990); *see also Rakas v. Illinois*, 439 U.S. 128, 143, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978) (the "capacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy") (citations omitted); *Illinois v. Andreas*, 463 U.S. 765, 771, 103 S.Ct. 3319, 77 L.Ed.2d 1003 (1983) (if a police investigation does not intrude upon a legitimate expectation of privacy, no "search" subject to the Fourth Amendment occurs).

A subjective expectation of privacy is legitimate for purposes of the Fourth Amendment only if it is "one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361, 88 S.Ct. 507 (Harlan, J., concurring). The reasonableness prong of the analysis in *Katz* is central to any Fourth Amendment analysis because the Amendment "reflects a choice that our society should be one in which citizens dwell in reasonable security and freedom from surveillance." *California v. Ciraolo*, 476 U.S. 207, 217, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) (quotation marks and citation omitted). Whether an expectation of privacy is reasonable

depends on "objective rules and customs that can be understood as reasonable by all parties involved." *Lucas v. S.C. Coastal Council*, 505 U.S. 1003, 1035, 112 S.Ct. 2886, 120 L.Ed.2d 798 (1992); *see also Rakas*, 439 U.S. at 143 n.12, 99 S.Ct. 421 ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society"). Although a person's home is generally a place where privacy may be expected, "objects, activities, or statements that he exposes to the plain view of outsiders are not protected because no intention to keep them to himself has been exhibited." *Katz*, 389 U.S. at 361, 88 S.Ct. 507 (Harlan, J., concurring) (quotation marks omitted).

"Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted." *Rakas*, 439 U.S. at 133-34, 99 S.Ct. 421 (quotation and citations omitted). Thus, in order to claim the protection of the Fourth Amendment, a defendant has the burden of demonstrating that he personally had an expectation of privacy in the place searched or the item seized, and that his expectation was reasonable. *Minnesota v. Carter*, 525 U.S. 83, 88, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (citing *Rakas*, 439 U.S. at 143 n.12, 99 S.Ct. 421).[5]

[5] Some state courts analyze whether a defendant "had a legitimate expectation of privacy under the rubric of 'standing' doctrine." *Carter*, 525 U.S. at 87, 119 S.Ct. 469. Colorado's Appellate Courts appear to be among those courts. *See, e.g.*, *People v. Nelson*, 296 P.3d 177, 182 (Colo.

B. Colorado Constitution

Like the Fourth Amendment, article II, section 7, of the Colorado Constitution protects a person's "legitimate expectations of privacy from unreasonable governmental intrusion." *People v. Oates*, 698 P.2d 811, 814 (Colo. 1985) (citations omitted). In determining the scope of the state constitutional provision, the Colorado Supreme Court has "employed the two-part test developed by Justice Harlan in his concurring opinion in *Katz*." *People v. Hillman*, 834 P.2d 1271, 1279 (Colo. 1992) (citation omitted). Thus, in analyzing an expectation of privacy claim, the Court inquires whether the defendant "has manifested a subjective expectation of privacy in the area, object, or activity subjected to the [governmental] intrusion and whether any such subjective expectation is one which society is prepared to recognize as reasonable." *Id.* (citation omitted); *see also People v. Rister*, 803 P.2d 483, 490 (1990) ("our approach in determining what kinds of seizures are 'reasonable' under article II, section 7, of the Colorado Constitution is similar to the approach taken by the United States Supreme Court").

App. 2012) ("Before a defendant can challenge the constitutionality of a search, he or she must establish that he or she has standing, which is a legitimate expectation of privacy in the areas searched or the items seized") (quotation and citations omitted). The United States Supreme Court takes a different approach. *See Carter*, 525 U.S. at 87, 119 S.Ct. 469 (noting that the Court in *Rakas* "expressly rejected" the standing analysis). The Court in *Carter* explained that central to the analysis in *Rakas* was "the idea that in determining whether a defendant is able to show the violation of his . . . Fourth Amendment rights, the 'definition of those rights is more properly placed within the purview of substantive Fourth Amendment law than within that of standing.'" *Id.* at 88 (quoting *Rakas*, 439 U.S. at 140, 99 S.Ct. 421).

On occasion, Colorado Courts have construed the search and seizure provision of the state constitution more broadly than the Fourth Amendment "in order to provide Colorado citizens with more protection against intrusions into their personal privacy than would be available under the Fourth Amendment to the United States Constitution." *Hillman*, 834 P.2d at 1279-80 (citation omitted); *see also People v. Dunkin*, 888 P.2d 305, 307 (Colo. App. 1994) ("In construing the Colorado constitution, our supreme court has in some cases imposed more stringent constraints on police conduct than those imposed by the United States Supreme Court in construing the federal constitution") (citations omitted). However, "in every case in which our supreme court has recognized a greater protection under the state constitution than that afforded by the federal constitution, it has identified a privacy interest deserving of greater protection than that available under the Fourth Amendment." *People v. Rossman*, 140 P.3d 172, 176 (Colo. App. 2006) (citations omitted).

II. The Defendant's Expectation of Privacy Claims

A. The Defendant's Profiles

The defendant posted his profiles on Match.com and AdultFriendFinder.com with the intent to make them accessible to other members of the websites. Furthermore, the AdultFriendFinder.com profile was apparently accessed directly

by TMZ and The Inquisitr, while the Match.com profile was forwarded to TMZ by another Match.com member.

More importantly, before law enforcement even applied for the records, the profiles had been published on the internet by both TMZ and The Inquisitr. This included the photographs posted and the tagline, "Will you visit me in prison?," which appeared on the profiles of both accounts. In other words, by the time the governmental intrusion took place, the profiles were already available to the public. Under these circumstances, the defendant cannot establish a subjective expectation of privacy—never mind a reasonable one—in the profiles. Even if a subjective expectation of privacy existed at some point, it was no longer present when law enforcement obtained his Match.com and AdultFriendFinder.com profile records.

Because the defendant failed to meet his burden of establishing a reasonable expectation of privacy in the profile records obtained by law enforcement from Match.com and AdultFriendFinder.com, the Court finds that those records are not protected by the Fourth Amendment or article II, section 7, of the Colorado Constitution. Therefore, to the extent that Motion D-117 seeks to suppress the defendant's profile records, it fails.

B. The Defendant's Subscription Information

1. United States Constitution

"[T]he Supreme Court [of the United States] has determined that the Fourth Amendment does not prohibit investigating officers from securing information revealed to a third-party without a warrant even if the information is revealed in confidence and on the assumption that it will be used only for limited purposes." *Dunkin*, 888 P.2d at 307 (citations omitted). Thus, the Supreme Court has found that there is no reasonable expectation of privacy in telephone and banking records under the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735, 742-45, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) (the government need not obtain a warrant to install a pen register to record numbers dialed from a telephone number because telephone customers do not have reasonable expectations of privacy in telephone numbers dialed); *United States v. Miller*, 425 U.S. 435, 442-43, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (a warrantless search of a bank customer's deposit information does not run afoul of the Fourth Amendment because bank customers do not have a reasonable expectation of privacy in banking transaction records voluntarily conveyed to bank employees).

In both *Miller* and *Smith*, the Court applied the *Katz* test and found that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44, 99 S.Ct. 2577 (citing, among

other cases, *Miller*, 425 U.S. at 442-44, 96 S.Ct. 1619). In *Miller*, the Court reasoned that the depositor "[took] the risk" that the information he submitted to the bank would be conveyed "to the Government," 425 U.S. at 443, 96 S.Ct. 1619, while in *Smith*, the Court reasoned that the telephone subscriber similarly "assumed the risk" that the information he provided to the phone company "would be divulged to the police," 442 U.S. at 745, 99 S.Ct. 2577.

The Court's research did not unearth any cases addressing whether a person has a reasonable expectation of privacy protected by the Fourth Amendment in subscription information he voluntarily submits or exposes to an internet dating company's administrator. However, the decision in *In re § 2703(d) Order; 10GJ3793*, 787 F. Supp. 2d 430 (E.D. Va. 2011), provides some guidance.

In *In re § 2703(d) Order*, the United States District Court for the Eastern District of Virginia held that records obtained by the government from a social networking site, containing petitioners' IP addresses and other subscriber information concerning petitioners' accounts, were not protected by the Fourth Amendment. *Id.* at 440. The Court concluded that petitioners had "voluntarily conveyed their IP addresses to the Twitter website, thus exposing the information to a third party administrator, and thereby relinquishing any reasonable expectation of privacy." *Id.* In so doing, the Court rejected petitioners' argument that *Smith* was distinguishable because "Twitter users do not directly, visibly, or knowingly

convey their IP addresses to the website, and thus maintain a legitimate privacy interest." *Id.* The Court noted that, "[b]efore creating a Twitter account, readers are notified that IP addresses are among the kinds of 'Log Data' that Twitter collects, transfers, and manipulates." *Id.* (citation omitted). Since petitioners had "voluntarily conveyed their IP addresses to Twitter as a condition of use, they [had] no legitimate Fourth Amendment privacy interest." *Id.* (citations omitted); *see also United States v. Warshak*, 631 F.3d 266, 287-88 (6th Cir. 2010) (extending Fourth Amendment protection to the contents of some email communications, but acknowledging that the internet service provider's notice of intent to monitor subscribers' emails diminished their expectation of privacy).

Here, the defendant voluntarily conveyed and exposed identification and billing information to two large social networking services. Furthermore, he voluntarily exposed his IP address to the administrators of both networks. Through his IP address, the website administrators were able to collect his log data, including log in times and the duration of sessions. There is no basis in the record to conclude that the defendant did not know that the websites would collect, monitor, transfer, and manipulate his log data.

Significantly, in recognition of the defendant's burden to establish a reasonable expectation of privacy, the Court afforded him an opportunity to present evidence on this issue. He declined to do so, and the record is barren of

any evidence—such as privacy terms and conditions of a website's membership—that would support a subjective expectation of privacy. Nor has the defendant presented any legal authority in support of his reliance on the Fourth Amendment to establish that his alleged expectation of privacy is reasonable.

Federal jurisdictions have rejected assertions of reasonable expectations of privacy under the Fourth Amendment with respect to subscriber information provided to an internet service provider. In fact, consistent with the rationale in *Smith* and *Miller*, "[e]very federal court to address th[e] issue has held that subscriber information provided to an internet [service] provider is not protected by the Fourth Amendment's privacy expectation." *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (citations omitted); *see also United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010) ("Federal courts have uniformly held that subscriber information provided to an internet [service] provider is not protected by the Fourth Amendment's privacy expectation because it is voluntarily conveyed to third parties") (quotation marks and citation omitted); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (holding the defendant could not establish a subjective expectation of privacy in his internet subscriber information, including his name, email address, telephone number, and physical address, because he "voluntarily conveyed" that information to the internet company, thereby "assum[ing] the risk" that the company would share that information with

law enforcement; even if he could show a subjective expectation of privacy in his subscriber information, "such an expectation would not be objectively reasonable") (quotation and citation omitted); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) ("We conclude that plaintiffs . . . lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators"); *United States v. Beckett*, 369 Fed. App'x. 52, 56 (11th Cir. 2010) (concluding that it was unreasonable for the defendant to have been unaware that his identifying information was being transmitted to the internet service providers; as such, he "assumed the risk" that the companies would reveal the information to law enforcement); *United States v. Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013) (because the defendant "chose to share pornographic files via a peer-to-peer network," he lacked an "expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers;" hence, the defendant "failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable") (quotation marks and citations omitted); *State v. Mello*, 27 A.3d 771, 775 (N.H. 2011) ("the overwhelming majority of federal and state courts that have addressed th[e] issue" have concluded "that a defendant has no reasonable expectation of privacy in subscriber information voluntarily provided to an Internet service provider") (citations omitted).

Based on the available legal authority and the record before it, the Court concludes that the defendant failed to demonstrate a legitimate expectation of privacy protected by the Fourth Amendment in the subscriber records obtained by law enforcement from Match.com and AdultFriendFinder.com. Accordingly, to the extent that his request to suppress subscriber records is grounded in the Fourth Amendment, it fails.

2. Colorado Constitution

As a preliminary matter, because both parties agree that the search and seizure provision of the Colorado Constitution and pertinent Colorado case law apply to the out-of-state documents obtained by law enforcement from Match.com and AdultFriendFinder.com, the Court assumes, without deciding, that such is the case. The Colorado Supreme Court has not directly addressed the issue, although it explained in *People v. Porter* that "the procedural rules of this jurisdiction" generally have "limited extraterritorial effect . . . absent denial of constitutional rights." 742 P.2d 922, 924 (Colo. 1987) (quoting *People v. Robinson*, 192 Colo. 48, 556 P.2d 466, 468 (Colo. 1976)). Relying on this language, a panel of the Colorado Court of Appeals determined in *People v. Taylor* that "if there was a violation of the defendant's Colorado constitutional rights"—as a result of the seizure by North Dakota officials of the defendant's phone records in that state pursuant to a search warrant issued by a North Dakota court—"then exclusion of

the evidence would be mandated even though the evidence may have been properly seized under the laws of the situs state." 804 P.2d 196, 198 (Colo. App. 1990).[6]

The Colorado Supreme Court has determined that the search and seizure provision of the Colorado Constitution "affords persons in this state a reasonable expectation of privacy in their personal telephone toll records and banking transaction records held by third-party banking and telephone service companies."

---

[6] There appears to be a split of authority on this issue. *Compare People v. Phillips*, 711 P.2d 423, 456 (Cal. 1985) (rejecting the defendant's suggestion "that evidence obtained in a manner that would not be proper in California, even if valid under federal law and the law of the state where it was obtained, should be excluded in California courts"); *Pooley v. State*, 705 P.2d 1293, 1303 (Alaska Ct. App. 1985) (holding "that the Alaska Constitution was not implicated here, even assuming that the [the California law enforcement agent's] conduct would have violated the Alaska Constitution if it had occurred in Alaska or had been engaged in by an Alaskan officer"); *McClellan v. State*, 359 So.2d 869, 873 (Fla. Dist. Ct. App. 1978) ("[E]vidence procured in a sister state pursuant to a search valid under the laws of that state is admissible in the trial of a criminal case in Florida notwithstanding that the warrant validly issued and executed in the sister state would not have been or was not valid under the laws of Florida; provided the warrant and its execution in the sister state does not offend U.S. Constitutional standards"); and *Young v. Commonwealth*, 313 S.W.2d 580, 581 (Ky. Ct. App. 1958) ("There can be no violation [of the search and seizure provision of the state constitution] except within the territorial limits of this state and by officers of this state"); *with State v. Cauley*, 863 S.W.2d 411, 416 (Tenn. 1993) ("When evidence is used in a Tennessee courtroom that has been obtained [in another state] at the behest of Tennessee authorities pursuant to their own investigation of a crime occurring within our borders . . . Tennessee's constitutional search and seizure principles should apply"); *State v. Torres*, 262 P.3d 1006, 1021 (Haw. 2011) ("We therefore conclude that, where evidence sought to be admitted in state court is the product of acts that occurred on federal property or in another state, by Hawai'i law enforcement officers or officers of another jurisdiction, due consideration . . . must be given to the Hawai'i Constitution and applicable case law"); *State v. Davis*, 834 P.2d 1008, 1012 (Or. 1992) (concluding that "[t]he standard of governmental conduct and the scope of the individual rights protected by [the search and seizure provision of the state constitution]" apply to "an out-of-state search by non-Oregon law enforcement officials"); *State v. Evers*, 815 A.2d 432, 441 (N.J. 2003) (the search and seizure provision of the state constitution "protects the rights of people within New Jersey from unreasonable searches and seizures by state officials, and its jurisdictional power extends to agents of the state who act beyond the state's borders in procuring evidence for criminal prosecutions in our courts").

People v. Mason, 989 P.2d 757, 759 (Colo. 1999) (citing *People v. Sporleder*, 666 P.2d 135, 141-42 (Colo. 1983), for the proposition that a telephone customer has a reasonable expectation of privacy in telephone numbers dialed; and *Charnes v. DiGiacomo*, 200 Colo. 94, 612 P.2d 1117, 1121 (Colo. 1980), for the proposition that a bank depositor has a reasonable expectation of privacy in a bank's records of his financial transactions).[7] Thus, notwithstanding *Miller* and *Smith*, the Colorado Supreme Court has found that, under the *Katz* test, there is a reasonable expectation of privacy in telephone records and banking records protected by the Colorado Constitution.

In *DiGiacomo*, the Court declined to follow the holding in *Miller*, reasoning that a customer "does not intend to forfeit" his expectation of privacy in records of his financial transactions by opening a bank account, "both because disclosure of information is incidental to the customer's main purpose, and because the use of banks is a business necessity and thus not entirely voluntary." *People v. Timmons*, 690 P.2d 213, 216 (Colo. 1984). Similarly, in *Sporleder*, the Court disagreed with the decision in *Smith* and "extend[ed] the rationale of *DiGiacomo* to pen registers." *Id.* "Paralleling the reasoning of [*DiGiacomo*]," the Court "found that telephone use is a necessity and that information supplied to the telephone company is merely

[7] "A minority of other states share [Colorado's] view." *Mason*, 989 P.2d at 759.

incidental to that necessity; therefore, no voluntary forfeiture of privacy occurs when a telephone is used." *Id.* (citing *Sporleder*, 666 P.2d at 141).[8]

The defendant relies on *Sporleder* and *DiGiacomo* to assert a state constitutional expectation of privacy in the subscriber information he provided or exposed to Match.com and AdultFriendFinder.com. *See* Reply at p. 2. These cases, however, are not dispositive.

Sporleder and *DiGiacomo* were decided thirty and thirty-three years ago, respectively. The Colorado Supreme Court recognized in 1999 that "the rapid advances in computer and telecommunications technology" since *Sporleder* and *DiGiacomo* may have changed "a person's reasonable expectations of privacy in telephone and bank records . . . so that ***the decisions may be subject to challenge***." *Mason*, 989 P.2d at 759 n.2 (emphasis added).[9] There have been numerous

---

[8] A year after deciding *Sporleder*, the Court found a reasonable expectation of privacy in telephone toll records. *See People v. Corr*, 682 P.2d 20, 27-28 (Colo. 1984).

[9] The decisions in *Sporleder* and *DiGiacomo* have not been immune from criticism. *See e.g.*, *People v. Haley*, 41 P.3d 666, 679 (Colo. 2001) (Kourlis, J., dissenting) (relying on Chief Justice Erickson's dissenting opinion in *Sporleder* and stating, "[i]n my view, it is not enough that a state supreme court differs with the United States Supreme Court"), *abrogated*, *People v. Esparza*, 272 P.3d 367 (Colo. 2012); *People v. McKinstrey*, 852 P.2d 467, 474 (Colo. 1993) (Rovira, J., specially concurring) ("I have repeatedly noted my disagreement with the development of different standards" in the area of "whether an intrusion is a search") (citations omitted); *Oates*, 698 P.2d at 822 (Erickson, C.J., dissenting) (In *Sporleder*, "I outlined in detail, by way of dissent, the reasons why a state court should be hesitant in interpreting nearly identical language in a state constitution to that in the federal constitution differently in an effort to reach a conclusion that is different from a square holding of the United States Supreme Court"). In *Oates*, Justice Rovira explained in his dissenting opinion that in neither *Sporleder* nor *DiGiacomo* "was there any review of the Colorado constitutional convention to ascertain whether the intent of the drafters of article II, section 7, was any different from that of those who

additional advances of great significance in computer and telecommunications technology since the Court made this comment fourteen years ago in *Mason*.[10]

More importantly, *Sporleder* and *DiGiacomo* are distinguishable. In *Sporleder*, the Court observed that "[a] telephone is ***a necessary component of modern life***. It is ***a personal and business necessity indispensable to one's ability to effectively communicate*** in today's complex society." 666 P.2d at 141 (emphasis added).[11] Likewise, in *DiGiacomo*, the Court agreed with the California Supreme Court's characterization of bank transactions as "***not completely voluntary*** because bank accounts are ***necessary to modern commercial life.***" 612

---

drafted the fourth amendment." *Id.* at 825 (Rovira, J., dissenting). In reaching those decisions, observed Justice Rovira, the Court did not engage in "any careful analysis of the text of article II, section 7, as compared to the text of the fourth amendment, which suggests or mandates that a different meaning should be ascribed to the Colorado constitutional provision." *Id.* Justice Rovira added that the Court in *Sporleder* and *DiGiacomo* did not undertake "any careful tracing of historical development to support the journey which the [C]ourt embarked on . . . ." *Id.* Hence, concluded Justice Rovira, the Court's "search for and discovery of more rights for individuals accused of criminal conduct under article II, section 7, than under the fourth amendment was not based on a thorough analysis of the Colorado Constitution." *Id.* Justice Rovira viewed the effect of the majority opinion in *Oates* as "continu[ing] the development of parallel and conflicting search and seizure law," and as "add[ing] another level of uncertainty to an already complex area of the law." *Id.* He feared that such conflict would "breed[] confusion on the part of law enforcement officers, and frustration and perplexity in the mind of the public as to what the law is." *Id.* As he eloquently put it, "[t]he law of search and seizure . . . is difficult enough to apply with but one line of authority to follow," namely, that of the United States Supreme Court, and when another line of authority is added under the state constitution, it "compounds the difficulty immeasurably." *Id.*

[10] The question whether an expectation of privacy in telephone and banking records continued to exist under the Colorado Constitution in 1999 was not before the Court and was not addressed in *Mason*. 989 P.2d at 759 n.2.

[11] The Court in *Sporleder* characterized as "somewhat idle" the discussion in *Miller* and *Smith* about "assuming risks" because, "as a practical matter, the telephone subscriber has no realistic alternative." 666 P.2d at 141 (citation omitted).

P.2d at 1121 (emphasis added) (citing *Burrows v. Superior Court*, 13 Cal. 3d 238, 529 P.2d 590, 596 (Cal. 1974).[12]

In stark contrast to the use of telephones and bank accounts—and arguably, certain uses of the internet—participation in a social network dating website is a completely voluntary activity; it is neither necessary to modern life nor indispensable to one's ability to effectively communicate.[13] Thus, whereas the Colorado Supreme Court was concerned in *Sporleder* and *DiGiacomo* with a customer's forfeiture of privacy in his telephone communications and financial records simply as a by-product of using a telephone or opening a bank account—necessary and even indispensable activities to modern life—in this case, the Court deals with information volitionally provided or exposed by the defendant as a result of signing up to be a member of two large social networking websites that have millions of members, a completely voluntary activity that is not necessary, much less indispensable, to modern life.

---

[12] Other than discussing the California Supreme Court's decision in *Burrows*, *DiGiacomo* contains very little legal analysis regarding a person's reasonable expectation of privacy in his bank records under the Colorado Constitution. 612 P.2d at 1121.

[13] Relying on *Sporleder*, the defendant asserted at the hearing that there is a reasonable expectation of privacy in general internet usage, an activity he views as a necessary aspect of modern life. But the question before the Court is not whether there is a reasonable expectation of privacy in any and all uses of the internet. The question before the Court is much narrower: whether there is a reasonable expectation of privacy in the specific use of an internet dating social networking service. Therefore, for purposes of the *Sporleder* analysis, the relevant inquiry is whether participation in internet dating is a necessary component to modern life.

Moreover, the Court in *Sporleder* noted that "[w]hen a telephone call is made, it is as if two people are having a conversation in the privacy of the home or office, locations entitled to protection under Article II, Section 7 of the Colorado Constitution." 666 P.2d at 141. The Court referred to the telephone as "an instrument of private communication." *Id.* at 142. As such, the Court was unwilling to find that a customer's "concomitant disclosure to the telephone company, for internal business purposes, of the numbers dialed" from a home phone somehow transformed the telephone subscriber's expectation of privacy into "an assumed risk" that the information would "be released to other persons for other purposes." *Id.* at 141.

While the information conveyed or exposed by the defendant to the administrators of Match.com and AdultFriendFinder.com may have been incidental to his main purpose, it is significant that his main purpose was not to have a private conversation through a private instrument from the privacy of his home or office; it was to have his identification and very personal information disseminated to other participants in the websites in order to secure a date or to start a relationship or a friendship. Whatever subjective expectation of privacy, if any, the defendant may have had when he chose to become a member of each dating website, he was presumably aware that there was a virtual certainty, not merely an assumed risk, that his identifying and personal information would be

released by the website's administrator to other persons in the social network. He also was presumably aware that he had no control over whether those persons would thereafter distribute his information to others within the network and to people outside the network without his consent or knowledge. Indeed, that may have happened the day after the shooting.[14]

Finally, in *Sporleder*, the Court held that a telephone subscriber does not lose his legitimate expectation of privacy in telephone numbers dialed from a home telephone as a result of the concomitant disclosure of those numbers to the telephone company. *Id.* at 140. Inherent in this holding is the determination that a telephone subscriber has a constitutionally protected expectation of privacy in phone numbers dialed from a home phone. In this case, the defendant failed to meet his burden of establishing an expectation of privacy, reasonable or otherwise, in the subscription information he disclosed or exposed to the administrators of Match.com and AdultFriendFinder.com. If, as part of his membership in those internet websites, he agreed to terms and conditions like the ones involved in *In re § 2703(d) Order*, no such expectation can exist. 787 F. Supp. 2d 430 (finding no legitimate Fourth Amendment privacy interest, and explaining that "[b]efore creating a Twitter account, readers are notified that IP addresses are among the kinds of 'Log Data' that Twitter collects, transfers, and manipulates").

[14] As indicated, the day after the shooting, one of the members of Match.com allegedly distributed the defendant's profile to TMZ without the defendant's consent or knowledge.

In sum, *Sporleder* and *DiGiacomo* are inapposite. Accordingly, the Court concludes that the defendant's reliance on these decisions is unavailing.

No Colorado case has addressed whether subscription information submitted to an internet dating service is protected by the Colorado Constitution. However, the decision in *Dunkin* is instructive.

In *Dunkin*, the Court held that, even if the defendants had a subjective expectation of privacy in their electrical utility records, "under the Colorado constitution, society does not view this expectation of privacy as a reasonable one." 888 P.2d at 308 (citation omitted). The Court in *Dunkin* relied on the Idaho Court of Appeals' decision in *State v. Kluss*, 867 P.2d 247, 254 (Idaho Ct. App. 1993), where the Court concluded that "'the scope of protection afforded by [the Idaho state constitution] [did] not extend to the individual power consumption records maintained by a utility' company because the defendant's expectation of privacy in such records was objectively unreasonable." *Id.* at 308 (quoting *Kluss*, 867 P.2d at 254). The *Dunkin* Court found persuasive the rationale in *Kluss*:

> In order to have electricity, Kluss was obliged to obtain the same from [the utility provider]. ***Kluss did nothing to create the records except consume power. The power records in the case at bar reveal only the amount of power usage. The power records were maintained by [the utility provider] in the ordinary course of business. They do not identify any activities of Kluss.*** On a comparative basis they may demonstrate that the power use at the Kluss home is greater or lesser than similar houses or at similar times or that the power use has increased or decreased at different times. ***The information does not provide any intimate details of Kluss's life, identify his friends or***

> ***political and business associates, nor does it provide or complete a 'virtual current biography.' The power records, unlike telephone or bank records, do not reveal discrete information about Kluss's activities.*** High power usage may be caused by any one of numerous factors: hot tubs, arc welders, poor insulation, ceramic or pottery kilns, or indoor gardening under artificial lights.

Id. (quoting *Kluss*, 867 P.2d at 254) (emphasis added).

As was the case in *Kluss*, other than providing identifying and payment information to Match.com and AdultFriendFinder.com, the defendant here did nothing to create the subscription records independently maintained in the regular course of business by those websites for their own purposes. Furthermore, like the power records in *Kluss*—which revealed the amount of power used, when power was used, increases or decreases in power usage, and how the power used compared to the power used at other households—the defendant's subscription records reveal log data, times of log in, the duration of log sessions, increases or decreases in usage, and how such use compared to use by other members. Neither the records in *Kluss* nor the defendant's subscription records include the content of any communications, let alone information about the subscriber's activities, intimate details of his life, his friends, his political and business associates, his religious orientation, or other discrete aspects of his life.[15]

[15] As indicated, the defendant disclosed some of this personal information on the profiles he posted on Match.com and AdultFriendFinder.com.

At the hearing, the defendant relied on the New Jersey Supreme Court's decision in *State v. Reid*. The Court in *Reid* found that, under the New Jersey state constitution, an individual has a privacy interest in his "IP address," as well as in any subscriber information he discloses to his internet service provider. 945 A.2d 26, 28 (N.J. 2008). The Court reasoned that, as a result of the large number of daily activities conducted on the internet, internet usage, which requires an IP address, is "integrally connected to essential activities of today's society." *Id.* at 33.

The Court is not bound by *Reid* and, in any event, finds that decision unpersuasive for several reasons. First, *Reid* involved an internet service provider, not an internet social networking service. In the Court's view, the instant case is more similar to *In re § 2703(d) Order*, 787 F. Supp. 2d 430, than it is to *Reid*.

Second, in finding a reasonable expectation of privacy, the *Reid* Court assumed that internet users are "unaware that a numerical IP address can be captured by the websites they visit." *Reid*, 945 A.2d at 33. Federal courts have declined to make the same assumption. *See e.g.*, *Beckett*, 369 F. App'x. at 56 (concluding that it was unreasonable for the defendant to have been unaware that his identifying information was being transmitted to the internet service providers). This Court likewise declines to make the assumption made by the *Reid* Court.

Lastly, *Reid* addressed the situation where an individual anonymously browses the internet. 945 A.2d at 33. Importantly, however, the Court recognized that an internet user may waive his expectation of privacy when he chooses to actively interact with a website by creating an account and revealing personal information. *See id.* at 33 n.2 (noting that internet users "may waive their expectation of confidentiality in any number of ways," such as by "identify[ing] themselves on a website when they make a purchase or complete a survey").[16] The privacy concern in question in *Reid*—to prevent "track[ing] a person's [general] Internet usage," *see id.* at 33—is different from the privacy claim raised by the defendant in this case. The records obtained by law enforcement from Match.com and AdultFriendFinder.com were generated because the defendant visited those social networking websites, created accounts, and voluntarily provided his personal information to those internet services. In other words, the defendant's actions exceeded the anonymous browsing activity at issue in *Reid*.

Under the circumstances present in this case, and on the record before it, the Court concludes that the defendant failed to demonstrate an expectation of privacy protected by the Colorado Constitution in the subscription records obtained by law

[16] The defendant not only identified himself when he signed up for AdultFriendFinder.com and Match.com, he specifically requested that his identification and very personal information be distributed to other members of the websites.

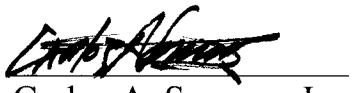
enforcement from Match.com and AdultFriendFinder.com. Therefore, the defendant's request to suppress those records on state constitutional grounds fails.

CONCLUSION

For all the foregoing reasons, the Court denies Motion D-117. The motion is denied as moot to the extent that the defendant seeks to suppress records from Match.com and AdultFriendFinder.com that contain communications with other members of those websites. The motion is otherwise denied based on the defendant's failure to establish a constitutionally protected expectation of privacy in the records he seeks to suppress.

Dated this 7th day of November of 2013.

BY THE COURT:



Carlos A. Samour, Jr.
District Court Judge

CERTIFICATE OF SERVICE

I hereby certify that on November 7, 2013, a true and correct copy of the **Order regarding defendant's motion to suppress evidence: records obtained from match.com and adult friend finder (D-117)** was served upon the following parties of record:

Karen Pearson
Amy Jorgenson
Rich Orman
Dan Zook
Jacob Edson
Lisa Teesch-Maguire
George Brauchler
Arapahoe County District Attorney's Office
6450 S. Revere Parkway
Centennial, CO 80111-6492
(via e-mail)

Sherilyn Koslosky
Rhonda Crandall
Daniel King
Tamara Brady
Kristen Nelson
Colorado State Public Defender's Office
1290 S. Broadway, Suite 900
Denver, CO 80203
(via e-mail)

Cheryl Robinson