Three Legal Considerations of Social Media and Email: Discovery, Privacy, Service of Process

Charlotte Winczer

Social Media

The purpose of social networking sites such as Facebook and MySpace is to provide an online environment for participants to share personal information about themselves with others in the context of social life and friendship. Users may not envision that an adversary in litigation would discover relevant material among their publicly posted information and request consent to access the private portions of their social networking sites for further discovery; and they may object on privacy grounds. The question of whether litigants have a legitimate reasonable expectation of privacy to material posted on social networking sites has been comprehensively addressed in *Romano v. Steelcase Inc*., 30 Misc.3d 426, 907 N.Y.S.2d 650.

In this personal injury action, the plaintiff, Ms. Romano, asserted that she could no longer participate in certain activities or that her enjoyment of life was affected as a result of the permanent injuries she suffered in the underlying incident. The defendant, Steelcase, claimed that the plaintiff's public postings on her MySpace and Facebook pages showed that she had an active lifestyle and traveled to Florida and Pennsylvania during the time period she claimed that her injuries prevented such activity. The plaintiff refused to provide the requested authorizations. *Id* at 429. Defendant moved for an order pursuant to CPLR 3101 to gain access to the plaintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information because there was a reasonable likelihood of discovering further evidence regarding her injuries that contradicted the plaintiff's claims for loss of enjoyment of life which was material and relevant to the defense's case. *Id* at 427.

In addressing the issue of privacy, the court pointed out: "In New York, there is no common-law right to privacy." *Id* at 432; and quoted *Katz v United States*, 389 US 347, 351 (1967): "The Fourth Amendment's right to privacy protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." In *United States v Lifshitz*, 369 F3d 173, 190 (2004) the Second Circuit explained: "Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient," in the

same way that someone sending a letter loses the expectation of privacy once the letter has been received. *Romano* at 433.

The court cited *Moreno v Hanford Sentinel, Inc*., 172 Cal App 4th 1125, 91 Cal Rptr 3d 858 (Ct App, 5th Dist 2009) which asserted that no one can have a reasonable expectation of privacy who proactively posts their writings on a social networking site making them open to public view available to anyone with a computer to see. In fact, MySpace reminds users that their profiles and MySpace forums are public spaces and Facebook permits users to select privacy options at their own risk, which may not be entirely protective. Therefore, the court reasoned the plaintiff has no legitimate reasonable expectation of privacy since Facebook and MySpace make no guarantee of complete privacy. *Romano* at 433, 434.

The court concluded that when the plaintiff created her social networking accounts she agreed to share her personal information with others regardless of her privacy settings, consistent with the nature and purpose of social networking sites. She could not claim to have a reasonable expectation of privacy because she knew that her information could become publicly available. "As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, '[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking.'" *Romano* at 434.

Complaint Against Facebook and Its Facial ID Recognition Technology

The Electronic Privacy Information Center (EPIC) and several other non-profit organizations filed a complaint with the Federal Trade Commission (FTC) against Facebook, the largest social network service in the United States, with approximately 150 million users. The petitioners are organizations involved with public interest issues of privacy and civil liberties, the impact of digital marketing on privacy and consumer welfare, and informational privacy at the state and federal levels. The main causes of action are: Facebook's implementation of facial recognition technology constitutes consumer harm and Facebook's use of facial recognition technology constitutes an unfair and deceptive trade practice.

Facial recognition technology is a method of digital biometric data collection that detects and identifies human faces. It was created when Facebook made changes to its photo technology in 2010 without obtaining users' consent. Users were encouraged to freely upload photos of themselves, friends and family. It works by generating a biometric signature for users who are tagged in photos on Facebook, i.e. using "summary data" from "photo comparisons." Facebook routinely encourages users to "tag," i.e. provide actual identifying information about themselves, their friends, and other people they may recognize. Facebook associates the tags with a user's account, compares what these tagged photos have in common, and stores a summary of this comparison.

Facebook enables "tag suggestions" by default, i.e. automated identification of facial images occurs in the absence of any user intervention. It is not possible for a user to delete the facial recognition data that Facebook has collected by following Facebook's instructions through the user's privacy settings.

Instead, the procedure for doing so is complicated and difficult; and it does not prevent Facebook from any further biometric data collection. While Facebook requires users to obtain consent before tagging a photo, it does not provide the technological means to do so and does not inform or remind users of this requirement. Furthermore, Facebook does not guarantee that advertisers, application developers, the government and other third parties would not be able to access "photo comparison data." In 2006 and 2007 Facebook made unauthorized disclosures of users' personal information and multiple federal lawsuits have ensued. In 2009 Facebook expanded the categories of personal information which it makes publicly available. In this regard EPIC and others filed a complaint with the FTC and millions of users have expressed their opposition to Facebook's policies through online groups and campaigns.

There is a genuine potential for violations of the Children's Online Privacy Protection Act (COPPA) through Facebook's facial recognition technology. As of May 2011, at least 7.5 million U.S. children under the age of thirteen actively used Facebook. This includes more than 5 million children under the age of ten. Facebook collects e-mail addresses and first and last names, which constitute personal information under COPPA, from each child with a Facebook account. Facebook's facial recognition technology links a user's photo summary data to the user's account, including the user's email address and first and last name. Because it is combined with other personal information, the photo summary data also falls within COPPA's definition of personal information. Facebook conditions a minor user's participation in photo sharing and tagging on the user's disclosure of photo summary data. Minors are at risk because they lack the capacity to consent to Facebook's Terms of Service and to understand the implications of disclosing personal information to Facebook.

The right of privacy is a personal and fundamental right in the United States. The privacy of an individual is directly impacted by the collection, use, and dissemination of personal information. The misuse of personal information may imperil the rights of due process and opportunities to obtain credit, employment, insurance and medical services. The excessive collection of personal data in the United States along with insufficient legal and technological protection has resulted in an increase in identity theft crime. The United States Supreme Court holding in *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989), cited in *Nat'l Cable & Tele. Assn. v. Fed. Commc'ns. Comm'n*, No. 07-1312 (D.C. Cir. Feb. 13, 2009) states: "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."

Unauthorized disclosure and/or public availability of their personal information places users at risk for commercial exploitation and exposure to possible public humiliation. The right of an individual to exercise control over their image in a commercial context is recognized in the Restatement (Second) of Torts § 652C (1977) which sets forth: "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."

In light of the extraordinary circumstances described above, EPIC and the other petitioners asked the FTC to investigate Facebook, determine the extent of harm to consumer privacy and safety, require Facebook to stop collection and use of users' biometric data without their affirmative opt-in consent, require Facebook to give users meaningful control over their personal information, establish appropriate security safeguards, limit the disclosure of user information to third parties and grant appropriate injunctive and compensatory relief.

E-service

In the *New York State Bar Association Journal* Vol. 85 No. 8, October 2013, John R. Higgitt discusses *The Emergence of "E-service" Under CPLR 308(5)* in his article with the same title. In *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306 (1950) the United States Supreme Court allowed the court broad discretion in devising an appropriate method of alternate service of process provided that it was reasonably calculated, under all the circumstances, to give the parties notice of the action. In New York, service affected by electronic processes, known as e-service, is a method of alternate service that courts have authorized under CPLR 308(5) in recent years. (Higgitt, 28-30)

E-service may be authorized by the court when the plaintiff demonstrates that service by the other methods provided in CPLR 308(1)-(4) is impracticable and the court determines that service of process by email is a means reasonably calculated to provide the defendant with notice of the action. Like other methods of alternate service, e-service should be considered cautiously because both the issues of impracticability and reasonableness may be challenged by a defendant who was subjected to the alternate service. If the challenge is successful, the statute of limitations may lapse before a new action can be commenced. E-service may be effective when it can withstand these challenges. (Higgitt 29, 30)

Several cases New York courts have recently decided involving e-service focus on reliability in establishing reasonableness; these include: *Hollow v. Hollow*, 193 Misc.2d 691 (N.Y. Sup. Ct. Oswego County Aug. 19, 2002), *Snyder v. Alternate Energy Inc.*, 19 Misc.3d 954 (Civ. Ct. N.Y.C. Apr. 4, 2008), *Alfred E. Mann Living Trust v. ETIRC Aviation S.A.R.L.*, 78 A.D.3d 137 (1st Dept. 2010), *Wang v. TIAA-CREFF Life Insurance Co.*, 2012 N.Y. Misc. LEXIS 5780 (N.Y. Sup.Ct. New York County Dec. 14, 2012), *Safadjou v. Mohammadi*, 105 A.D.3d 1423 (4th Dept. 2013).

These decisions indicate that alternate service by email under CPLR 308(5) is allowable under *Mullane* if a plaintiff can show that the defendant is reasonably likely to receive the email. The reliability of an email address for an alternate method of service of process can be established by showing that: (1) a defendant themself used the address to receive email, and that they had done so recently, or (2) a defendant has acknowledged a particular address as theirs and that they likely use that address to receive email. Specific details that should be evaluated when considering alternate service by email are:

To which email address or addresses must the process be sent?

What message must be placed in the subject line of the email?

> What text must be placed in the body of the email? How many times must the email be sent, and over what period of time? Who can (or cannot) send the email? What documents should be attached to the email? In which format must the documents be attached to the email? (Higgitt 31)

In granting alternate service by email, a court may be wise to require another of the more familiar methods of alternate service in conjunction with it, e-service-plus, as an additional protection against a reasonableness challenge. (Higgitt 30, 31)

In *Fortunato v. Chase Bank USA, N.A.*, 2012 U.S. Dist. LEXIS 80594 (S.D.N.Y. 2012) the United States Court for the Southern District of New York permitted Chase Bank to implead the plaintiff's daughter, Nicole. However, the court rejected Chase Bank's request for alternate service on the daughter by email to an address found on her Facebook page for failure to substantiate the likelihood that the third party defendant would receive the impleader service at the email address given. The court reasoned:

> Chase has not set forth any facts that would give the Court a degree of certainty that the Facebook profile its investigator located is in fact maintained by Nicole or that the email address listed on the Facebook profile is operational and accessed by Nicole. Indeed, the Court's understanding is that anyone can make a Facebook profile using real, fake, or incomplete information, and thus, there is no way for the Court to confirm whether the Nicole Fortunato the investigator found is in fact the third-party Defendant to be served. *Id* at 7, 8.

Perhaps a court may authorize alternate service to a party's Facebook page if the reliability of the email address as discussed above can be demonstrated in the context of the reasonableness requirement under *Mullane* (Higgitt 32).

Work Cited

Higgitt, John R. "The Emergence of 'E-Service' Under CPLR 308(5)." *New York State Bar Association Journal* 85 (2013): 28-35. Print.

Nominating faculty: Professor Marissa Moran, Law 4704, Department of Law and Paralegal Studies, School of Professional Studies, New York City College of Technology, CUNY.

Cite as: Winczer, C. (2014). The legal considerations of social media and email: Discovery, privacy, service of process. *City Tech Writer, 9,* 18-22, Online at https://openlab.citytech.cuny.edu/city-tech-writer-sampler/