Up, Periscope: Mobile Streaming Video Technologies, Privacy in Public, and the Right to Record

Daxton R. Stewart  
*Texas Christian University, d.stewart@tcu.edu*

Jeremy Littau  
*Lehigh University, jjl409@lehigh.edu*

Follow this and additional works at: [http://preserve.lehigh.edu/cas-journalism-faculty-publications](http://preserve.lehigh.edu/cas-journalism-faculty-publications)

Part of the [Journalism Studies Commons](http://preserve.lehigh.edu/cas-journalism-faculty-publications), and the [Social Media Commons](http://preserve.lehigh.edu/cas-journalism-faculty-publications)

**Recommended Citation**

[http://preserve.lehigh.edu/cas-journalism-faculty-publications/5](http://preserve.lehigh.edu/cas-journalism-faculty-publications/5)

This Article is brought to you for free and open access by the Journalism at Lehigh Preserve. It has been accepted for inclusion in Faculty Publications by an authorized administrator of Lehigh Preserve. For more information, please contact preserve@lehigh.edu.
Up, Periscope: Mobile Streaming Video Technologies, Privacy in Public, and the Right to Record

Manuscript submitted to Journalism and Mass Communication Quarterly Special Issue: Information Access and Control in an Age of Big Data June 1, 2015

Dr. Daxton R. "Chip" Stewart
Associate Dean and Associate Professor
Bob Schieffer College of Communication
Texas Christian University
TCU Box 298040
Fort Worth, Texas 76129
d.stewart@tcu.edu

Dr. Jeremy Littau
Assistant Professor
Weinstock Center for Journalism
Lehigh University
33 Coppee Drive
Bethlehem, Pennsylvania 18015
jjl409@lehigh.edu

Dr. Stewart earned his Ph.D. in Journalism at the University of Missouri; his LL.M. in Dispute Resolution at the University of Missouri; and his J.D. at the University of Texas.

Dr. Littau earned his Ph.D. in Journalism at the University of Missouri.

Keywords: Privacy, live streaming, mobile streaming video technology, social media, right to record, First Amendment, Meerkat, Periscope, privacy in public, obscurity
When mobile apps Meerkat and Periscope launched in early 2015, with them came even more possibilities for opening the public sphere to constant video broadcast on easily accessible platforms. These live streaming technologies, which allow smartphone users to broadcast real-time video directly to followers, are the most recent encroachment on the waning notion that people may have some right to privacy in public places.

These apps gained immediate popularity upon their release. Meerkat was the breakout success in March 2015 at the influential South by Southwest Interactive festival in Austin (Isaac, 2015). The app received an immediate challenge when Twitter launched a similar live streaming app, Periscope, less than a month later and saw it become one of the top 30 iPhone app downloads in its first week (Kuittinen, 2015). While live streaming video apps are not new, widespread growth in the use of this technology had been limited by poor quality and lack of social connectivity. Meerkat and Periscope represent a breakthrough, with society-wide implications. Former presidential spokesperson Dan Pfeiffer predicts that as citizens and journalists increasingly become their own broadcasters, these kinds of live streaming apps will affect the 2016 presidential election in ways similar to Twitter’s influence on the 2012 campaign and Facebook’s influence in 2008 (Pfeiffer, 2015). Citizen reporters have used recorded video in past campaigns to document candidate gaffes, campaign rally controversies, or private conversations that go public. Pfeiffer suggests that these controversies and gaffes take on a different character when it becomes live video (2015).
Mobile streaming video technology (MSVT) seen in such apps as Meerkat or Periscope is certainly not the only significant technological advancement with effects on privacy in recent years, but it is potentially transformative in that these technologies open the public sphere to constant, democratized monitoring. Until recently, such monitoring has been the province of closed-circuit television (CCTV) systems, such as security cameras set up by private businesses and law enforcement in major cities such as London, New York, Chicago, and Boston (Kelly, 2013; Manjoo, 2013). Rather than a closed-circuit video stream available to businesses and government, however, MSVTs make broadcasting the public sphere as easy as downloading and installing a free app on one’s smartphone and tapping the screen; the only cost is the drain on one’s monthly data plan. Unlike CCTV, the purpose of MSVTs is not law enforcement or terrorism prevention; rather, they exist to allow users to share the world around them. Periscope CEO Keyvon Beykpour noted the uses from the day the app launched, varying from "a hot air balloon witnessing sunrise in Cappadocia, Turkey" to "probably 60 people Periscoping the same fire from different angles" after an explosion in Brooklyn (Herrmann, 2015).

While Meerkat and Periscope have faced some legal scrutiny in the area of copyright after massive live streaming of content such as episodes of HBO’s Game of Thrones (Jarvey, 2015) and the pay-per-view boxing match between Manny Pacquiao and Floyd Mayweather (Sandomir, 2015), they have as yet received little attention for their potential to invade privacy. Both Beykpour and Meerkat founder Ben Rubin have suggested that their apps do not create an inappropriate intrusion into the public sphere. As Rubin noted, "Think of the selfie culture these days."
Culturally, we've reached a point where cameras are more familiar and people have started to feel comfortable with video" (Isaac & Goel, 2015). Beykpour commented that by developing a live streaming app many years after other technologies had shifted people's expectations of privacy, "there are still legitimate questions but for the most part, the world has accepted that these capabilities exist" (Sydell, 2015).

Acceptance of the existence of these technologies, however, does not necessarily signal that people have surrendered any expectation of privacy as MSVT use grows. In her approach to privacy harms as violations of the contextual integrity of personal information, Nissenbaum (2009) noted:

The rapid transformations we have witnessed in socio-technological systems brought about by computing and information technologies has often thrust change upon people and societies without a careful evaluation of harms and benefits, perturbations in social and cultural values, and whether and by whom these changes are needed or wanted...By the time these ruptures surface in public deliberation, protest, or court cases, the new normal may be comfortably entrenched, but far from comfortably accepted (p. 160-61).

Further complicating the law surrounding use of MSVTs is the right of citizens and journalists to record video in public places. Under United States law, taking photographs in public places has increasingly received protection under the First Amendment, though courts are split on the extent to which those protections should be extended to recording video (Kreimer, 2011).

The purpose of this article is to examine this tension between people's expectations of privacy in public when MSVTs are widely available and the law of
privacy, which has evolved little in the digital era. Do people have any legal remedies when they are unwillingly the subjects of a live stream? To what extent is use of MSVTs to record and stream video protected under the First Amendment? This study uses legal research methodology to examine court decisions and statutes relevant to these issues as well as the work of legal scholars to chart a course for understanding the law surrounding MSVTs.

**Broadcasting and Mobile Streaming Video Technologies**

The process of shooting video and making it available for public consumption can happen several different ways, and its process is a matter of both technology and distribution. Consider the differences between television broadcasts and Internet video. Network and pay television have traditionally distributed video product via channels on a one-to-many broadcast format that sends video to consumers via over-the-air transmission, cable wires, and satellite signal (Driscoll & Dupagne, 2014). But the technology aspect involves how that video is acquired and processed as well. Television channels have the option of broadcasting recorded and edited video for news, entertainment, and commercials, but the channels also can broadcast video live and in real-time. The technology, signal transmission, regulation, and licensing costs all contribute to high barriers to entry that make it difficult for everyday citizens to compete in traditional broadcast video, whereas corporations have the resources to handle these costs (Picard & Chon, 2004).

Internet video, on the other hand, has fewer barriers to entry. Larger corporate broadcasters have used recorded video in the form of video file formats to distribute via the Internet, but they also have had the resources to distribute in real-
time online. (Papagiannidis & Berry, 2006). This latter method, known as "over-the-top" streaming video, allows users to view video of an event much as they would watch a live broadcast on television, but via a website or mobile application on a phone or tablet or by television on an Internet streaming box such as AppleTV or Roku (Sherman & Waterman, in press). Conversely, Internet video distribution has become more democratized as technology has improved because costs have declined sharply as technology has gotten simpler and more portable. Video hosting services such as YouTube and Vimeo have allowed smaller journalism operations and average people to post recorded video files available for viewing by anyone online (Burgess & Green, 2013). Thus the growth of online video streaming in the past five years has slowly allowed citizen players to compete alongside broadcast corporations (Monterde & Postill, 2014; Foth et al., 2014), but the idea of streaming video with low barriers for entry had largely remained elusive.

Mass video streaming technology actually has been available since the late 1990s, with companies such as RealPlayer pioneering the use of mass webcasts that made a single broadcast available to multiple personal computer users at the same time (Hardawar, 2013). The technological challenge and cost meant that even large broadcast companies contracted with third-party services such as MLB Advance Media to deliver streaming video (Brown, 2014). For citizen creators, streaming video production and distribution has come in various forms over the past five years, with notable competitors being Ustream, Justin.tv, and Google Plus’ “Hangouts Live” option. Ustream separated itself from the others by using mobile phone technology for capturing and sending video to the Internet, unlike the others
that relied on webcams installed in personal computers. But even these three main players were plagued by problems such as poor video quality, slow upload speeds, and lack of high-quality cameras on mobile phones and personal computers (Lee, 2015a).

The launch of Meerkat and Periscope represented a leap forward in everyday distribution of streaming video. Meerkat and Periscope were combining for about 70,000 links to live video per day just two months after launch (Topsy, 2015). The potential creator pool is young, with 50% of people age 18-34 indicating an interest in trying the apps (Adweek, 2015). These apps, along with Ustream’s offering, are more generally conceptualized for this article as Mobile Streaming Video Technologies (MSVT), which are differentiated from other streaming video types that comes in that they use mobile technology such as phones or tablets to both capture and distribute streaming video.

While it is important to understand that Meerkat and Periscope represent another technological iteration of existing MSVT, their emergence as mass-use products is significant because they have added a social network layer (Allen, 2015). Periscope offers a good example of how this works, as a consumer can discover Periscope streams in two ways. The first is via Twitter link; the person streaming video can tap a button to post a link to that video feed on Twitter, so if a Twitter user is following someone who is using Periscope and posting links, they have access to that stream. The second is through notifications tied to social network following. People can socially connect to a user on Periscope similar to how they do so on Facebook or Twitter and in fact with Periscope the process involves
automatically following anyone a person follows on Twitter as well, such that building a large, connected audience of watchers requires little effort. These social connections allow for phone notifications that report when a Periscope followee is streaming video. With notifications a person can shift between live streams from followers similar to switching channels on a television, except in the case of streaming video these "channels" go live and then disappear when a user starts or stops streaming (Pullen, 2015).

Meerkat and Periscope represent a technological improvement in MSVTs as well because of their function. The apps allow for real-time conversation and allow users to save their video even after the stream is over, meaning video can be uploaded to a video service such as YouTube (Bereznak, 2015), and Periscope also allows a person to view a video within the app for a short length of time even after the stream has stopped (Wagner, 2015). Both of these new MSVT apps also have been lauded for their simplicity and perceived higher quality compared to Ustream (Taube, 2015). Viewers can leave comments as they watch, and this feedback shows up on screen while a person broadcasts. This creates a type of two-way interaction, in which a camera operator can read messages and respond with audible voice (Lee, 2015b).

In sum, MSVTs are best understood as something akin to broadcast television with two major differences. First, their use of mobile phones to capture and stream good, quality video mean that anyone, anywhere has the ability to become a live video broadcaster so long as they have a capable smartphone, and this represents a significant change in the barriers for entry to live streaming. Second, dissemination
of this video is highly decentralized along social network lines, meaning the power to capture audience attention for events such as news has shifted away from the singular format of the television channel such that it now includes distribution along social networks.

Users of all types are using MSVTs. Journalists have been quick to adopt both Meerkat and Periscope, which can turn any reporter into a type of broadcast journalist regardless of their usual medium (Tompkins, 2015). Online and print reporters have embraced this ability to broadcast events live in real time, such as prayer vigils in Ferguson, Missouri (Oremus, 2015), doctor-journalist Sanjay Gupta performing surgery live, and a journalist showing what it is like to do live interviews (Lee, 2015b). There also have been incidents of citizen journalists using the apps to report in real time, including coverage of a building fire and collapse in New York City (Lever, 2015) or arrests in progress that turned into alleged intimidation by police (Carney, 2015). In addition, brands and companies have embraced live streaming tools.⁴

Privacy as a Legal Concept

Privacy is a core value shared among human communities⁵ that is, as Nissenbaum described, "among the rights, duties, or values of any morally legitimate social and political system" (2009, p. 66). In Western democracies, unlike totalitarian states, society relies "on privacy as a shield for group and individual life," not just in politics but also in family, religious, and other personal affairs, with roots in notions of individualism, involvement in associations, and civil liberties
protecting citizens from power exercised by government or private interests (Westin, 1967, p. 23). While the word "privacy" does not appear in the U.S. Constitution, it is recognized by people as a fundamental interest: "The right to privacy, it seems, is what makes us civilized" (Alderman & Kennedy, 2005, p. xiv).

In the past decade, scholars have begun to untangle the web of interconnected concepts and principles embedded in the law of privacy. This article draws most heavily from the work of two of influential privacy law concepts developed in the past decade that focus on privacy harms: Nissenbaum’s (2009) examination of "contextual integrity" and Solove’s (2008) "taxonomy of privacy."

Nissenbaum (2009) recognizes that standards of privacy have not necessarily changed as technology has advanced; rather, that the kinds of threats to those standards have changed, leading to schisms between people’s expectations and their experiences. As such, privacy harms are caused when the advancement of technology clashes with people’s "context-relative informational norms" (Nissenbaum, 2009, p. 148). For instance, in considering a technology similar in some ways to MSVTs, Nissenbaum found the development of Google Street View to be a violation of contextual integrity because the images were personally identifiable, provided information about people’s whereabouts, and were out of the control of the people they concerned (p. 219).

Context is also important to Solove (2008), who focused on disruptions to human activities caused when their notions of privacy are improperly protected. Two of the "harmful activities" he identified were in areas of "information collection" and "information dissemination" (p. 103). Information collection, such as
government wiretapping or CCTV systems, may be problematic to individuals and to society when constant monitoring causes general anxiety, fear of embarrassment, discourages participation in groups, or otherwise leads to self-censorship.

Information dissemination, on the other hand, is more concerned with the release of gathered personal information or data, by breaches of confidentiality or other inappropriate disclosures.

When Solove developed this taxonomy in 2008, there was a clear divide between information collection and information dissemination, which were typically distinct activities. What is novel about MSVTs, at least regarding the challenge they present to privacy law, is that these activities may now be done concurrently, on a large scale, by anyone with a smartphone. Unlike photo and video sharing social media tools such as Instagram, Vine, and YouTube, the stream is generated in real time and requires no upload. As Trevor Hughes of the International Association of Privacy Professionals noted, live streaming apps "create situations where the editorial pause that currently exists -- where you can think about what you're posting before you post it -- goes away" (Sydell, 2015). This immediacy, combined with widespread affordability and accessibility of live streaming apps, brings about the intersection of two privacy areas that previously were considered to be distinct, and increase the potential for harm that cannot be undone.

Examining these requires looking at two important privacy concepts, privacy in public and the right to record, to determine any potential civil liability that users of MSVTs may face when people's context-relative informational norms are
challenged when these areas of information collection and dissemination happen at the same time.

**Privacy in Public**

When Warren and Brandeis authored their seminal treatise "The Right to Privacy" in 1890, shaping the way jurists and scholars would view an individual’s right to privacy in the twentieth century, the photography and telephone technology involved was much more limited in its ability to pry into one’s private life in public places. Warren and Brandeis established a basis for areas in which people should be able to sue for damages for harm done to their "right to be let alone." Left out of this conceptualization was any notion of a right to privacy in public places; rather, these were "to protect the privacy of private life, and to whatever degree and whatever connection a man’s life has ceased to be private...to that extent the protection is likely to be withdrawn" (Warren & Brandeis, 1890, p. 214).

Prosser (1960) identified these harms as "privacy torts," legal rights existing outside of traditional contract and property law that could result in successful lawsuits when deprived through actions such as trespassing, misappropriation of one's image or likeness, or publishing one's private matters such as letters. Most relevant to the discussion of privacy in public is the tort Prosser identified as "intrusion upon seclusion," which provides a remedy to people who have their private lives harmed through technological means such as hidden cameras or recording devices without their knowledge or consent in a way that would be highly offensive to a reasonable person. The intrusion tort does not require publication,
instead resting on the principle that the act of intrusion itself is harmful (Fowler v. Southern Bell Telephone, 1965, p. 155). But Prosser noted that the intrusion tort includes a caveat similar to that described by Warren and Brandeis: “On the public street or in any public place, the plaintiff has no right to be let alone, and it is no invasion of his privacy to do no more than follow him about” (Prosser, 1960, p. 391).

This was at odds with other American notions of privacy in public. Westin (1967), for example, saw this as a kind of anonymity occurring "when the individual is in public places or performing public acts" but nevertheless should be free from monitoring and scrutiny:

> He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of behavior and role that would operate if he were known to those observing him. (p. 31)

At least one court in this era had an opportunity to consider the issue of constant, private surveillance. Consumer advocate Ralph Nader sued General Motors, alleging invasion of privacy, in part because General Motors had kept him under surveillance for extended periods of time, including having its agents follow him into a bank to see how much money he was withdrawing. The Court of Appeals of New York suggested that "mere observation" of Nader in public places would not be actionable, though it also opined that "(a) person does not make public everything he does merely by being in a public place," and thus, "under certain circumstances, surveillance may be so 'overzealous' as to render it actionable," suggesting that
following him into a bank may be enough to trigger liability (Nader v. General Motors Corp, 1970, p. 771).

Nevertheless, as technology advanced into the digital age with widespread surveillance and monitoring in public places, the law did not advance the notion that people may indeed retain some privacy in public. During the rise of digital photography and the World Wide Web in the 1990s, scholars recognized the potential for increased privacy harms and called for enhanced protection for individuals against intrusion of this sort. McClurg (1995) suggested that courts recognize "public intrusion" as a tort, noting that "(t)ort law clings stubbornly to the principle that privacy cannot be invaded in or from a public place," and instead should recognize harm caused by intrusion that is "highly offensive to a reasonable person" and would also consider the defendant’s motive in gathering that information and the extent to which it was disseminated (p. 1087). Lidsky (1998), also recognizing the advancement of surveillance technology and its increased use by journalists, proposed rejuvenating the tort of intrusion by making privacy in public possible while also recognizing a newsgathering privilege for matters of legitimate public interest. As she noted:

If the intrusion tort is to shield plaintiffs from prying, spying, and lying by the media, courts must interpret the tort more expansively. Courts must acknowledge that citizens are entitled to a modicum of privacy even in public places, and must modernize the intrusion tort to respond to the threat posed by high-tech surveillance methods (p. 248).
These standards, however, have not been adopted by courts or legislatures, even as technology advanced to the modern capabilities preceded by MSVTs. Nissenbaum noted that video surveillance in public may be a "lost cause" because it is "so commonplace now that objections are increasingly difficult to carry against the force of the reasonable expectation, against what I regard as the 'tyranny of the normal'" (2009, p. 160-61).

As such, any right to privacy in public remains elusive in modern American jurisprudence. Courts typically have connected modern privacy rights in a person's "reasonable expectation of privacy," a term borrowed from Fourth Amendment jurisprudence regarding government power to conduct searches in criminal investigations (Kerr, 2007). Outside of that context, courts have been reluctant to find a reasonable expectation of privacy or, as intrusion torts require, highly offensive conduct in connection with an individual's actions in public. When homeowners challenged the Google Street View program on grounds of intrusion and other torts, for example, the U.S. Court of Appeals for the Third Circuit dismissed the lawsuit, finding that "(n)o person of ordinary sensibilities would be shamed, humiliated, or have suffered mentally as a result of a vehicle entering into his or her ungated driveway and photographing the view from there" (Boring v. Google, 2010, p. 279). Even information overheard in less publicly open spheres such as workplaces may not provide a reasonable expectation of privacy if the person could expect to be seen or to have others overhear those conversations (Kemp v. Block, 1985).
If there is an exception to this limitation of tort collection for acts committed in public, it may be found in what Strahilevitz (2005) has identified as the doctrine of "limited privacy." For example, in a case involving a secret recording made by a journalist of a "telepsychic" working for a pay-per-minute phone service, the California Supreme Court found that employees working at that office, while they may expect to be overheard by other employees, may also reasonably expect not to have those conversations recorded and broadcast to the public (Sanders v. ABC, 1999). This focused on the harm caused by the dissemination of the recording, which in the context of MSVTs would be unavoidable. However, this case appears to be an outlier and is likely confined to California's interpretation of its state's law of privacy.

Considering the aforementioned background on the law of intrusion upon seclusion, it is hard to conceive of a way in which live streaming would lead to civil liability if used in public places. Just as live television or radio broadcasts from public places would not lead to liability for privacy violations on intrusion grounds, MSVTs would be unlikely to open a new avenue of tort collection for those claiming harm unless the intrusion upon seclusion tort were to be revised or rejuvenated by legislatures or courts.

**Rights to Photograph and Record Video in Public**

Complicating people's ability to protect any privacy in public from recording and streaming by MSVTs is the First Amendment, which has provided robust protection for photography that courts have in some instances extended to video
recording. Challengers have invoked the First Amendment to strike down laws that would restrict the ability to take photographs in public places, even when those laws may have non-objectionable public policy behind them. For example, in *Ex parte Ronald Thompson* (2014), the Texas Court of Criminal Appeals struck down the state’s "Improper Photography" law, which had made it illegal for a person to photograph, videotape, or otherwise electronically record or broadcast an image of another person without consent and "with intent to arouse or gratify the sexual desire of any person" (Texas Penal Code, 2014).9

The court described the inherent expressive nature in creating photographs and visual recordings and held that the statute was unconstitutionally overbroad, essentially applying "to any non-consensual photograph, occurring anywhere" as long as the intent to gratify sexual desire was present. It went on to note that the law "could easily be applied to an entertainment reporter who takes a photograph of an attractive celebrity on a public street" (Ex parte Ronald Thompson, 2014, p. 350).

This decision -- broadly protecting a person’s right to record video or take photographs in public places under the First Amendment -- is just one of a line of court decisions that provide substantial support to users of MSVTs. However, the U.S. Supreme Court has yet to recognize a clear right under the First Amendment to make audio or video recordings in public places. And in the age of what Kreimer (2011) termed "pervasive image capture," courts have not provided consistent, clear guidance on the rules on recording or capturing photographs in public places.

Kreimer found that a “a solid line of courts has recognized that image capture can claim protection under the First Amendment” (2011, p. 368), pointing out four
U.S. Circuit Court of Appeals courts that have recognized such rights. Other circuits have been less supportive of rights to record. For example, when a man was arrested for carrying a tape recorder to a Ku Klux Klan rally in Lafayette, Indiana, he argued to police that his recording of a public event like this should be protected under the First Amendment, but he was told that only journalists were allowed to bring recording devices, and he was arrested when he continued toward the rally area (Potts v. City of Lafayette, 1997). The city argued that police believed he may use the recording device as a weapon "to injure attendees" by throwing it; meanwhile, members of the press were allowed "to take in pens, paper, and tape recorders (as) a reasonable accommodation of their First Amendment rights" (p. 1109-12). The U.S. Court of Appeals for the Seventh Circuit supported the city in this case, opining that "there is nothing in the Constitution which guarantees the right to record a public event" (p. 1111).

As the reach of digital technology has advanced, however, state and federal appeals courts have had a slightly more expansive view of rights to record under the First Amendment in the context of eavesdropping and wiretapping laws. In A.C.L.U. v. Alvarez (2012a), the Seventh Circuit found the Illinois eavesdropping law deficient upon a challenge by the American Civil Liberties Union, which had created a public program encouraging citizens to record the activities of police officers. The court stood by its decision in Potts v. City of Lafayette, though it noted that any "right to gather information may be limited under certain circumstances," which in the case of Potts involved potentially throwing a tape recorder as a weapon (A.C.L.U. v. Alvarez, 2012a, p. 591). Upon remand, the district court agreed, striking down the
law narrowly as it applied to the ACLU’s police recording program (A.C.L.U. v. Alvarez, 2012b).

Where the Seventh Circuit appears to have drawn the line between Potts and the A.C.L.U. cases was in the distinction between making a recording -- which it said was clearly protected under the First Amendment in the A.C.L.U. case -- and having the right to do so in a public place, which it said could be curtailed as circumstances required:

The act of making an audio or audiovisual recording is necessarily included within the First Amendment’s guarantee of speech and press rights as a corollary of the right to disseminate the resulting recording. The right to publish or broadcast an audio or audiovisual recording would be insecure, or largely ineffective, if the antecedent act of making the recording is wholly unprotected...By way of a simple analogy, banning photography or note-taking at a public event would raise serious First Amendment concerns; a law of that sort would obviously affect the right to publish the resulting photograph or disseminate a report derived from the notes. The same is true of a ban on audio and audiovisual recording (A.C.L.U. v. Alvarez, 2012a, p. 595-96).

The U.S. Court of Appeals for the First Circuit similarly found First Amendment protection for recording police activity in public places, with facts perhaps more relevant to users of MSVTs. A man was arrested under the Massachusetts’ wiretapping law for using his cell phone to record Boston police arresting another person; after the charges were dismissed, he filed suit against the city for violating
his civil rights (Glik v. Cunniffe, 2011). The First Circuit agreed with his argument, emphasizing the importance of protecting citizens’ right to record public officials: "The filming of government officials engaged in their duties in a public place, including police officers performing their responsibilities, fits comfortably within (First Amendment) principles" (p. 82). In 2015, a federal court for the Southern District of New York found that this right to record police was "clearly established" by other circuit courts of appeal to the point that police could expect that they would be recorded and thus could be liable for violating a journalist’s First Amendment rights (Higginbotham v. City of New York, 2015).

Rather than a broad First Amendment right to record, though, these courts appear to have limited their holdings to recording of a certain type or in a certain place. The Southern District of New York found that even this right to record police in public came with limits; "(f)or instance, it may not apply in particularly dangerous situations, if the recording interferes with the police activity, if it is surreptitious, if it is done by the subject of the police activity, or if the police activity is part of an undercover investigation" (p. 19).

Several states currently allow some form of civil liability or criminal punishment for unauthorized recording in less public places. According to the Digital Media Law Project (2014), 11 states require all parties to a conversation to consent to its recording. California, for example, makes it a crime to eavesdrop on a "confidential communication" through any technological or recording device punishable by a fine of up to $2,500, though it "excludes communication made in a public gathering" (California Penal Code, 2015). Florida has a similar law, making
such recording a third degree felony without making a specific exemption for 
recording made in public places (Florida Statutes, 2014). When former presidential 
candidate Mitt Romney was recorded making his infamous "47 percent" statement 
to a group of supporters in 2012, it is likely that the recording -- made secretly by a 
person attending the event, which did not allow journalists -- violated the Florida 
law on recording (Romm, 2012). An MSVT used to broadcast in this situation would 
be likely to trigger violations of similar recording statutes.

It is hard to reconcile holdings recognizing a robust right to take photographs 
or record video in public under the First Amendment as found by Texas' highest 
court of criminal appeals with decisions by other federal appeals courts limiting the 
right to record to only certain activities of police and public officials in public places. 
While recent cases seem to favor a right to record -- and, by extension, likely a right 
to broadcast via MSVTs -- in public places, there is still no definitive precedent 
people can turn to in more general cases not involving public officials or police 
officers.

As such, the door is at least slightly open for Congress and state legislatures 
to consider laws that could punish the act of recording without knowledge or 
consent or provide civil remedies to citizens suffering privacy harms caused by the 
act of recording inherent in MSVTs. However, the advance of First Amendment-
based protection for photography and video recording in cases such as Ex parte 
Circuit make any new regulation likely to face legitimate challenges in court when 
the regulation is aimed at anything occurring in public places. Further, such
restrictions would conflict with the newsgathering and public information benefits of MSVTs, which enrich citizens in democracy and provide a valuable check on state power as journalism becomes more a product of its citizens than of institutional and corporate sources.

**Conclusion**

As drone technologies were becoming more accessible to consumers, Calo (2011) suggested that drones would serve as a "privacy catalyst," helping privacy law develop after decades in which it had "clearly stalled" (p. 29). Indeed, by September 2014, 13 states had passed civil or criminal laws "specifically to block unwanted aerial surveillance from privately owned, unmanned aircraft" (Bennett, 2014) and the Federal Aviation Administration had proposed numerous regulations on drone use (Shane, 2015). In a similar manner, MSVTs also have great potential to be privacy law catalysts, as legislatures and courts consider the balance between people’s right to record and live stream, or any potential right to be free from being recorded and streamed, in public places.

It is not difficult to imagine that MSVTs could, for example, be integrated with drones, adding an additional potentially intrusive element of live, private surveillance gathered from above. Further, while Meerkat and Periscope began as iPhone-based MSVTs, it is plausible that they will become available on connected wearable computing technologies such as watches, jewelry and glasses, making the act of recording even less noticeable by those having their actions captured and disseminated. Thierer (2015) noted that the "tort of intrusion upon seclusion may
evolve in response" to increased surveillance in connection with such advances in wearable technologies (p. 102). Such adjustments, which would likely involve embracing the "limited privacy" approach Strahilevitz (2005) identified, are one avenue in which plaintiffs may have some recourse for violations of their expectation of privacy, even in public places.

If basing liability on the act of information collection does not provide an avenue for legal action for unwilling subjects of MSVTs, and if the First Amendment continues to develop as a bar on states from making the act of recording in public unlawful, then the focus may need to shift to the distribution portion of live streaming. In this area, the emerging doctrine of obscurity holds some potential.

The U.S. Supreme Court recognized obscurity when it held that a convicted felon maintained a personal privacy interest in his FBI rap sheet, a compilation of a person’s state and federal arrests and convictions, in ruling that the Department of Justice did not have to release it upon a request from a journalist under the federal Freedom of Information Act (Department of Justice v. Reporters Committee for Freedom of the Press, 1989). The court found that "the privacy interest maintaining the practical obscurity of rap-sheet information will always be high" (p. 770) because of the personal information contained, and it was satisfied that the public interest would be served because the information contained in rap sheets was already a matter of public record around the country. The harm was in the increased accessibility of these records because the spread of the information beyond expected boundaries allows the information to "readily be exploited for
purposes other than those for which it was originally made publicly accessible” (Solove, 2008, p. 150).

The resulting doctrine of practical obscurity has been oft-criticized, called "mythological" regarding notions of privacy in public (Anderson, 2012) and "misguided" in the context of public records (Kirtley, 2015). But obscurity has been more embraced in discussions about online interactions. Hartzog & Stutzman (2013) conceptualized obscurity as "a state of unknowing" (p. 5) and see it as a general expectation in online behavior. For example, as social media have evolved, one trend is for Internet users to migrate toward activities that can make their communications more obscure, such as the ephemeral photo service Snapchat, which "can delete information within seconds after the recipient views it" (Selinger & Hartzog, in press, p. 3). Further, obscurity is a natural fit for reining in expansive surveillance powers of government, argue Hartzog & Selinger (in press), who suggest that the proper balance to protect individual rights may be to make surveillance "hard but possible" (p. 4).

In the context of MSVTs, obscurity is not about the act of being left alone in public. Rather, it is about reasonably being able to expect that one's public life will not be open to immediate, worldwide online viewing and archiving without any potential remedy. As Nissenbaum (2009) noted in the context of Google Street View, "even if something occurs in a public space or is inscribed in a public record there may still be powerful moral reasons for constraining its flow" (p. 217).

The First Amendment, of course, makes such constraining extremely difficult through the law. Preventing content such as video streaming from being
disseminated would be a prior restraint, which American courts soundly rejected in a line of 20th century cases.\textsuperscript{12} As Chief Justice Warren Burger wrote for the Supreme Court majority that overturned a lower court's gag order, "prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights" (Nebraska Press Association v. Stuart, 1976, p. 559).

In Europe, one potential remedy to shut down a live stream or an archived version of something captured by MSVT would be analogous to the "right to be forgotten" established in the Google Spain SL v. Agencia Espanola de Proteccion de Datos case (2014), which allows people to seek court orders to remove information about themselves from being linked to by Internet search engines. However, obscurity law in the United States is as yet unable to extend this far because the First Amendment prevents courts from issuing such takedown orders (Larson, 2013). Similar challenges would face efforts to pass legislation requiring facial blurring or other remedies available in Canada and Australia that arose in the context of Google Street View (Nissenbaum, 2009).

The primary legal obstacle facing those seeking to avoid the scrutiny of MSVTs remains overcoming the notion that something done in public may never again be private. For now, under United States law, users of MSVTs are unlikely to face civil or criminal liability for their use. Further development of intrusion upon seclusion law and the doctrine of obscurity are two potential avenues in restoring balance to notions of privacy.
References

A.C.L.U. v. Alvarez (2012a), 679 F. 3d 583 (7th Cir.).


Florida Statute (2014), 934.03.

Fordyce v. City of Seattle (1995), 55 F. 3d 436 (9th Cir.).


Fowler v. Southern Bell Telephone and Telegraph Co. (1965), 343 F.2d 150, 155 (5th Cir.).


Glik v. Cunniffe (2011), 655 F. 3d 78 (1st Cir.).


Iacobucci v. Boulter (1999), 193 F. 3d 14 (1st Cir.).


28


Potts v. City of Lafayette (1997), 121 F. 3d 1106 (7th Cir.).


Smith v. City of Cumming (2000), 212 F. 3d 1332 (11th Cir.).


Tunick v. Safir (2000), 228 F. 3d 135 (2nd Cir.).


---

1 Consider an early instance of Meerkat use by a journalist, which illustrates subjective privacy harm with the potential of objective harm. David Weigel of Bloomberg was using Meerkat to live-stream an appearance before the press by Senator Rand Paul after delivering a speech. While the senator himself had used Meerkat before, he expressed concerns "about what streaming video could do to the interactions between a senator with endless portfolios, and voters with endless and unpredictable obsessions" before suggesting that he preferred not to have his one-on-one interactions with voters live streamed because, as the senator put it, "If we know that every interaction with every voter is going to be filmed, it'll mean that you have plastic candidates saying nothing" (Weigel, 2015).

2 For example, live streaming was possible for organizations such as the non-profit *Texas Tribune*, which broadcast the closing moments of the 2013 legislative session, including Wendy Davis' filibuster of a contentious abortion bill, on YouTube (Stelter, 2013).

3 For example, during the Occupy Wall Street protests in New York City in 2011 and 2012, journalist Tim Pool became recognized as one of the most important sources of coverage after live streaming on Ustream from his smartphone (Fox, 2011).

4 The San Francisco Giants were the first Major League Baseball team to use live streaming to supplement broadcasts, showing pregame warmups and festivities while waiting for the actual television broadcast to go live (Vernon, 2015). Other brands such as Mountain Dew used MSVTs to showcase events sponsored by the
company, a type of real-time marketing effort generated from mobile (Morrison, 2015).

5 The roots of privacy may very well predate humanity in the animal world, in which "virtually all animals have need for the temporary individual seclusion or small-unit intimacy that constitute two of the core aspects of privacy" (Westin, 1967, p. 10).

6 Google Street View is a program in which cameras mounted on vehicles capture images from public streets; these are then uploaded into an easily accessible and searchable Google maps program.

7 In one foundational case in this context, the U.S. Supreme Court held in that a person engaged in illegal gambling over a telephone line had a reasonable expectation of privacy in a phone booth in a public place (Katz v. U.S., 1968). More recently, the court found reasonable expectations of privacy in not having a global positioning system (GPS) device placed on one's automobile without a warrant (U.S. v. Jones, 2012) and in the items on one's cell phone that was seized incident to an arrest (Riley v. California, 2014). However, the logic underlying this has not been easily extended to civil lawsuits for intrusion. For example, the Supreme Court had an opportunity to weigh in on a police officer's expectation of privacy in his department-issued pager, on which he had transmitted a number of improper text messages that led to his firing, but the court declined to make a sweeping statement about "reasonableness" of the officer's expectation in this instance (Quon v. City of Ontario, 2014).

8 As yet, courts have not distinguished between a right to record and a right to broadcast under the First Amendment, likely because the ability has been limited to institutional broadcasters typically regulated by the Federal Communications Commission. While streaming via MSVT may trigger a distinction between these activities, this article does not seek to treat them as separate. The difficulty under the First Amendment in regulating dissemination of video, whether live or recorded, is discussed in the conclusion of this article.

9 The man who challenged the law had been charged with 26 counts of improper photography, mostly involving young girls in swimsuits at the water park portion of SeaWorld in San Antonio.


11 The Illinois eavesdropping law carved out an exception for live broadcasting "by radio, television, or otherwise" of public events, which the court in dicta suggested was perhaps "broad enough to cover recordings made by individuals as well as the institutional press" (A.C.L.U. v Alvarez, 2012b, p. 604). Such an exemption would have likely covered MSVTs if the law had not been struck down.

12 For example, striking down Minnesota's nuisance law that had allowed a court to shut down publication of a newspaper (Near v. Minnesota, 1931) and rejecting government requests to enjoin publication of news stories based on the Pentagon Papers (New York Times v. United States, 1971).