Legal and Ethical Implications of Mobile Live-Streaming Video Apps

Abstract
The introduction of mobile apps such as Meerkat, Periscope, and Facebook Live has sparked enthusiasm for live-streaming video. This study explores the legal and ethical implications of mobile live-streaming video apps through a review of public-policy considerations and the computing literature as well as analyses of a mix of quantitative and qualitative user data. We identify lines of research inquiry for five policy challenges and two areas of the literature in which the impact of these apps is so far unaddressed. The detailed data gathered from these inquiries will significantly contribute to the design and development of tools, signals or affordances to address the concerns that our study identifies. We hope our work will help shape the fields of ubiquitous computing and collaborative and social computing, jurisprudence, public policy and applied ethics in the future.

Author Keywords
Mobile live-streaming video; security; informatics; privacy; surveillance; intellectual property.

ACM Classification Keywords
K.4.0 [Computers And Society]: General.
Introduction
Live-streaming video is surging, attributable to the 2015 introduction of mobile apps Meerkat and Periscope [48, 49] and leaps in mobile streaming technology [21], which has sparked growth and user enthusiasm for the medium [31, 35, 37]. Facebook in 2016 has delved into the technology with its Live platform [32]. A Cisco White Paper estimates that by 2017, video will account for 30% of all internet traffic and 70% of mobile traffic [36, 50].

Live-streaming apps give rise to numerous legal and ethical concerns around privacy [28] and information sharing [39], publicity and intellectual property [11, 34, 37], and have implications in the U.S., the European Union and elsewhere for legislation and other forms of public policy as well as community and cultural norms and individual actions [18, 27]. Users exulting “Wow, I can do this!” as they point their smartphones and broadcast live to the world may not have asked, as a researcher posed in another context [17], “Wait, can I do this?” or even “Should I do this?” Parallels can be drawn to the new contexts and affordances for legal and ethical concerns with video provided by the spread of internet-connected smartphones featuring high-quality cameras [38], wearable cameras such as the GoPro or Google Glass [3, 4], dashboard cameras [52] and other hands-free video devices. These technologies have sparked debates regarding owners’ legal rights to film others in various settings as well as who may view these videos and what is captured by the devices [1, 24, 28, 39].

Our review of public-policy considerations and the computing literature has led us to identify lines of research inquiry for five public-policy challenges and two areas of the literature in which the impact of these apps is so far unaddressed. We set forth these questions to help guide future work in the fields of ubiquitous computing and collaborative and social computing, jurisprudence, public policy and applied ethics. We also describe our plans for an explanatory, sequential mixed-methods study on familiarity with and attitudes about mobile live-streaming video and related legal and ethical issues among likely users and bystanders to the technology.

Unaddressed Policy Questions
Citizen videographers in conflict with police
In several recent cases, private citizens in the U.S. who pulled out their smartphones to record police actions were themselves arrested [12, 22]. Such cases have been on the upswing in the wake of several high-profile recordings of violent police actions against African-Americans, such as the death of Eric Garner [12]. Many such arrests have been struck down due to U.S. law’s protection of free speech and against unreasonable search and seizure, as in the 2011 Glik v. Cunniffe decision [22]. However, police have invoked obstruction, resisting arrest or other charges to justify actions against citizen videographers [12].

- How might increased familiarity with and usage of live-streaming apps impact debate and policies regarding such recordings?

Surveillance norms
Devices such as “nanny cams,” laptop cameras, modern closed-circuit video systems and other small, unobtrusive wireless recorders have given members of the general public an unprecedented ability to put others under surveillance without their explicit knowledge or consent [9]. While recordings of nannies or other types of employees, rental occupants and guests via hidden cameras in homes or on other private property is generally allowed under U.S. federal and state laws, some
Voyeurism
Another concern is that of voyeurism, defined as the “act of filming or disseminating images of a person’s private areas under circumstance in which the person had a reasonable expectation of privacy regardless of whether the person is in a private or public area” [see 1, p. 8]. Notable examples include surreptitious “upskirt” and “downblouse” videos [2]; and “revenge porn,” in which spurned intimate partners post explicit video of their former partners for viewing by strangers online [6]. Video voyeurism also can be legal entertainment as well as big business. Adult video distribution and consumption will likely continue as the largest such category of internet entertainment and enterprise [47]. Two other categories of multimillion-dollar entertainment ventures for live video streaming are gaming and sports [11].

- How much of a threat do these apps pose to intellectual property for sports, the arts and other entertainment?

Global differences in legal concepts
International privacy laws are generally modeled on schemes that focus on individuals’ rights to their information, such as the European Union’s Data Protection Directive or the OECD Guidelines and Privacy Framework, or on those that center on actual or potential harm from disclosure, such as the Asia-Pacific Economic Cooperative (APEC) [45]. A notable exception is the U.S., where...
confidentiality and data security are protected by a “patchwork quilt” of federal and state laws [45, p. 74].

U.S. courts have also held that individuals have a right to publicity. This is defined as the right to “prevent the unauthorized commercial use of an individual’s name, likeness, or other recognizable aspects of one’s persona” and “gives an individual the exclusive right to license the use of his or her identity for commercial promotion” [41]. This is similar to the Latin American concept known as “habeas data,” generally defined as the right of an individual to petition a court to help take action against any third party to help safeguard the individual’s image, privacy, honor and freedom of information [45].

In 2014’s Google v. Gonzalez, the E.U. Court of Justice established another data-protection right: the “right to be forgotten.” This requires Google to remove posts referencing individuals from search results within E.U. jurisdiction upon request [42].

Mobile live-streaming video seems to pose challenges similar to those of ephemeral mobile messaging apps such as Snapchat for the archiving, discovery and analysis of electronically stored information (“ESI”) during U.S. civil litigation [15, 26]. The increased capability for individual point-of-view video streams may help buttress witness credibility and establish timelines through geo-location metadata and the distinctive quality of the video [3, 15].

Unaddressed Questions in the HCI Literature

Why, who and what in privacy and surveillance

In 2004, Bohn et al. [5] attempted to classify the social, economic and ethical implications of ubiquitous technologies. They noted the usefulness in this context of Harvard law professor Lawrence Lessig’s four motives for personal privacy: as empowerment, as utility, as dignity, and as a regulating agent. These motives help define why privacy is desirable beyond protecting individual freedom in a democracy, in the authors’ view [5] and were drawn on by Fiesler et al. for investigations into legal and ethical issues regarding fan fiction [16, 17, 18].

Bohn et al. also highlighted Gary T. Marx’s concepts of “border crossings”: natural borders, social borders, spatial or temporal borders, and “borders due to ephemeral or transitory effects” [5, p. 12]. The authors noted that a boundary violation concerns who does it and what is happening. This echoes Goffman’s concept of impression management via “front stage” and “back stage” [20]. But studies have not addressed these issues in the context of mobile live-streaming video.

- How do mobile app bystanders’ notions of privacy and boundary violations change according to why, who or what is being live-streamed via a mobile phone?
- How might these notions impact the design or implementation of mobile live-streaming video apps?

Defining and designing for legal and ethical concerns

Denning et al. [10] conducted ethnographic-style research into the privacy perspectives of bystanders to augmented reality (AR) devices by observing and interviewing N=31 near a mock AR device. Echoing Bohn et al., these bystanders noted that what was being recorded made a difference in their perceptions [10] and wanted to be
asked for permission to record them and to have the ability to block transmission [10]. The results were used to map design concepts for privacy-mediating technologies [10]. This is congruent with Erickson and Kellogg's work in designing for social transluence [13].

To teach concepts of ethics in remote video surveillance, Danielson [9] proposed a stylized two-player game between the roles of Viewer and Viewed, in which each has the choice to Reveal Camera or Conceal Camera [9]. Another game proposed by Danielson, RoboCops & Citizens, uses team tournament-style play to simulate Innocent Events, Hostile Events or Aid Events [9]. However, Danielson failed to anticipate the impact that social media would have on video in such contexts.

The inadequacies of various Terms of Service in notifying users of their rights and responsibilities, let alone providing meaningful ability to consent, has caused scrutiny [25, 35, 40, 44, 46]. However, efforts such as the "Terms of Service; Didn't Read" project have not yet devised a solution that is targeted for mobile users [46].

Zhang et al.’s Kaleido system would prevent unauthorized recording at a theater by sabotaging the appearance of on-screen images captured by a video camera, while keeping image quality high for those watching in person [51]. A similar solution might work for mobile apps, while still preserving a smartphone owner’s ability to live-stream video in legally and ethically sound contexts.

- What recommendations can be made for mobile phone handset design and for the design of software to help address identified concerns of likely users of and bystanders to mobile live-streaming video apps?

- Are there other opportunities to address these concerns specifically for mobile users in non-technical contexts, such as for training or education?

**Future Work**

Our team is conducting an explanatory, sequential mixed-methods study into the following two research questions:

- What can a recent survey of likely app users and bystanders tell us about familiarity with mobile live-video technologies and attitudes about online sharing?
- How do bystanders react “in the wild” to the presence of mobile live-streaming video in two differing social/spatial contexts: a large public gathering space and a small, semi-private meeting space?

In order to answer these questions, we will first collect and analyze data from an online survey of N>100 likely users of social media and messaging apps to assess their familiarity with and attitudes about issues with mobile live-streaming video. We then plan to conduct in situ observations of and semi-structured interviews with bystanders to the simulated use of these apps “in the wild” in two contexts: a crowd of sports fans and other passersby outside a stadium on a university campus, and a social gathering in a residential building’s common area.

**Significance and Broader Impacts**

The detailed data gathered from these inquiries will significantly contribute to the design and development of tools, signals or affordances to address the concerns that our study identifies. We hope our work will help shape the fields of ubiquitous computing and collaborative and social computing, jurisprudence, public policy and applied ethics in the future.
The questions provoked by our work also apply to the "Internet of Things," [29] also known as social devices, as well as to the evolving areas of augmented [4] and virtual reality [1, 14]. We hope these inquiries will be taken up by scholars researching design practices [43] and usage of these emerging technologies to address concerns with privacy, surveillance and related issues in the future.

References


