
Legal and Ethical Implications of Mobile Live-Streaming Video Apps

Cori Faklaris

Francesco Cafaro

Sara Anne Hook

Asa Blevins

Matt O'Haver

Neha Singhal

Department of Human-Centered Computing,
School of Informatics and Computing,
Indiana University-Purdue University Indianapolis,
535 W. Michigan St., Indianapolis, IN, USA 46202
cfaklari@iupui.edu
fcafaro@iu.edu
sahook@iupui.edu
asablevins@gmail.com
maohaver@iupui.edu
singhneh@uemail.iu.edu

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
MobileHCI '16 Adjunct, September 06-09, 2016, Florence, Italy
© 2016 ACM. ISBN 978-1-4503-4413-5/16/09...\$15.00
DOI: <http://dx.doi.org/10.1145/2957265.2961845>

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.

This is the author's manuscript of the article published in final edited form as:

Faklaris, C., Cafaro, F., Hook, S. A., Blevins, A., O'Haver, M., & Singhal, N. (2016). Legal and Ethical Implications of Mobile Live-streaming Video Apps. In Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct (pp. 722–729). New York, NY, USA: ACM. <https://doi.org/10.1145/2957265.2961845>

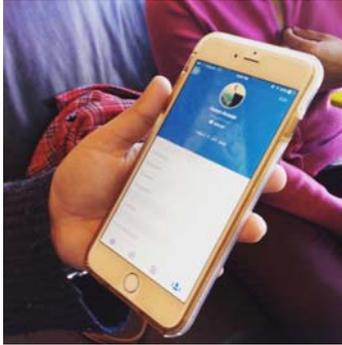


Figure 1: The Periscope mobile live-streaming app has gained many fans since its introduction in 2015. Photo by the authors.



Figure 2: In early 2016, Facebook began making a big push for its new Live product, led by media organizations and personalities. Image by the authors.

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



Figure 3: A screenshot of a Periscope broadcast of the Mayweather-Pacquiao boxing match in 2015. Image by the authors.

caveats apply: first, that the recording be video only, as those involving audio generally violate federal wiretapping laws [7]; and second, that such recordings be limited to common areas and not bedrooms or bathrooms, where a more absolute expectation of privacy holds [7]. In some cases, surveillance devices may be welcomed if and when its subjects become explicitly aware of them and benefit from their existence. Examples include video conferencing and security systems for home or business [9, 39].

- *How might wiretapping laws be best reformed to account for mobile video that carries audio?*
- *How can individuals be aided in opting out of such recordings?*

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].

- *What, if any, need exists for statutes to address crimes such as voyeurism that are committed in the use of mobile live-streaming video apps?*

Live-event piracy

Mobile apps for live-streaming video have sparked additional issues with gaming, sports and other content considered intellectual property (“IP”), the domain of copyrights, patents, trademarks and trade secrets [40]. Professional sports leagues were the first to take note of the potential for Meerkat, Periscope and similar apps to disrupt the ability to make money from live events. Live television rights and ticket sales are main drivers of revenue for professional sports leagues. The increasing accessibility of video and live streaming capability for individuals, as opposed to broadcast and cable television networks, has long posed a threat to these revenue streams [11, 36]. For the 2015 boxing match between Floyd Mayweather and Manny Pacquiao, it was estimated that more than 10,000 people viewed just one Periscope stream instead of spending money for broadcasts [30]. Although sports enterprises may have power under U.S. law as well as financial motivation to block such streams [11], they may also seek to harness the platforms themselves for broadcasting and to engage with fans on social media [30]. The advent of 360-degree video cameras makes this use case even more compelling [14].

- *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].

- *How are variously defined rights of privacy, publicity and other policy and litigation issues being impacted by the rise of mobile live-streaming video apps?*

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 translucence [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

1. Barfield, W., ed. 2015. *Fundamentals of wearable computers and augmented reality*. CRC Press.
2. Bell, V., Hemmens, C., and Steiner, B. 2006. Up skirts and down blouses: A statutory analysis of legislative responses to video voyeurism. *Criminal Justice Studies* 19.3: 301-314.
3. Bergman, K. 2014. Cyborgs in the Courtroom: The Use of Google Glass Recordings in Litigation. *Rich. JL & Tech.* 20: 11-14.
4. Bilton, N. 2012. Google Begins Testing Its Augmented Reality Glasses. Retrieved May 10, 2016 from <http://bits.blogs.nytimes.com/2012/04/04/google-begins-testing-its-augmented-reality-glasses/>
5. Bohn, J., et al. 2005. Social, economic, and ethical implications of ambient intelligence and ubiquitous computing. In *Ambient intelligence*, W. Weber, J.M. Rabaey, E. Aarts, eds. Springer Berlin Heidelberg, 5-29. <https://dx.doi.org/10.1007/b138670>
6. Citron, D.K., and Franks, M.A. 2014. Criminalizing revenge porn. *Wake Forest Law Review* 49: 345.
7. Coble, C. 2015. Is a Surveillance Camera in the Guest Room an Invasion of Privacy? Retrieved Feb. 17, 2016 from http://blogs.findlaw.com/law_and_life/2015/07/is-a-surveillance-camera-in-the-guest-room-an-invasion-ofprivacy.html?DCMP=cfeatures
8. Creswell, J.W. 2013. *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications, Inc.
9. Danielson, P. 2002. Video surveillance for the rest of us: Proliferation, privacy, and ethics education. In *IEEE Symposium on Technology and Society (ISTAS'02)*, 162-167. <http://dx.doi.org/10.1109/ISTAS.2002.1013812>
10. Denning, T., Dehlawi, Z., and Kohno, T. 2014. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy mediating technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*, 2377-2386. <http://dx.doi.org/10.1145/2556288.2557352>
11. Edelman, M. 2015. From Meerkat to Periscope: Does Intellectual Property Law Prohibit the Live Streaming of Commercial Sporting Events? *Columbia Journal of Law & the Arts*, Vol. 39, No. 4. Retrieved Feb. 17, 2016 from <http://ssrn.com/abstract=2661875>
12. Eltman, F. 2015. Citizens taking video of police increasingly finding themselves facing arrest, advocates say. Retrieved Feb. 15, 2016 from <http://www.startribune.com/policesometimes-turn-on-the-citizen-with-a-smartphonevideo/323317251/>
13. Erickson, T., and Kellogg, W.A. 2000. Social translucence: an approach to designing systems that support social processes. In *ACM transactions on computer-human interaction (TOCHI)* 7.1: 5983.
14. Faklaris, C. 2015. Can virtual reality be a 'killer app' for journalists to tell great stories? Retrieved Feb. 15, 2016 from <http://www.ibj.com/articles/53396-faklaris-can-virtualreality-be-a-killer-app-for-journalists-to-tell-greatstories>
15. Faklaris, C., and Hook, S.A. 2016. Oh, Snap! The State of Electronic Discovery Amid the Rise of Snapchat, WhatsApp, Kik and Other Mobile Messaging Apps. *Federal Lawyer*, May 2016, 64-75.

16. Fiesler, C. 2007. Everything I need to know I learned from fandom: How existing social norms can help shape the next generation of user-generated content. *Vand. J. Ent. & Tech. L.* 10: 729.
17. Fiesler, C., and Bruckman, A.S. 2014. Remixers' understandings of fair use online. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing (CSCW '14)*, 1023-1032.
<http://dx.doi.org/10.1145/2531602.2531695>
18. Fiesler, Casey, et al. 2015. Ethics for studying online sociotechnical systems in a big data world. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing (CSCW '15)*, 289-292.
<http://dx.doi.org/10.1145/2685553.2685558>
19. 5 legal tips for Periscope users. 2015. Retrieved Feb. 17, 2016 from
<http://lizerbramlaw.com/2015/07/28/5-legal-tips-forperiscope/>
20. Goffman, E. 1959. *The Presentation of Self in Everyday Life*. Doubleday Anchor Books.
21. Harris, R. 2016. App Publishers Can Now Easily Add Mobile Live Video Streaming to iOS and Android Apps. Retrieved March 8, 2016 from
<https://appdeveloper magazine.com/3667/2016/2/24/App-Publishers-Can-Now-Easily-Add-Mobile-Live-Video-Streaming-to-iOS-and-Android-Apps>
22. Hampton, C. 2011. Confirmation of a Catch-22: Glik v. Cunniffe and the Paradox of Citizen Recording. *Fla. L. Rev.* 63: 1549.
23. Henry, A. 2015. The Best Live Streaming App for Android. Retrieved Feb. 17, 2016 from
<http://liferhacker.com/the-best-live-streaming-app-for-android-1731698249>
24. Henry, A. 2015. The Best Live Streaming App for iPhone. Retrieved Feb. 17, 2016 from
<http://liferhacker.com/the-best-live-streaming-app-for-iphone-1746655285>
25. Hern, Alex. 2015. I read all the small print on the Internet and it made me want to die. Retrieved Feb. 17, 2016 from
<http://www.theguardian.com/technology/2015/jun/15/iread-all-the-small-print-on-the-internet>
26. Hook, S.A., and Faklaris, C. 2015. Social Media, The Internet and Electronically Stored Information (ESI) Challenges. National Business Institute, Altoona, WI.
<https://scholarworks.iupui.edu/handle/1805/7177>
27. Hopkins, E. 2015. How Periscope Could Be Used for Context Delivery. Retrieved Feb. 17 2016 from
<http://mediashift.org/idealab/2015/06/how-periscopecould-be-used-for-context-delivery/>
28. Meerkat, Periscope, Privacy and the Law: 10 Expert Tips For Legal Live Streaming. 2015. Retrieved Feb. 17, 2016 from
<http://www.influencerchat.com/2015/06/legal-livestreaming/>
29. Internet of Things Global Standards Initiative. International Telecommunications Union. Retrieved Feb. 17, 2016 from <http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx>
30. Kanno-Youngs, Z.V. 2015. Sports league keeping an eye on Periscope, Meerkat. Retrieved Feb. 16, 2016 from
<http://www.usatoday.com/story/sports/2015/08/24/periscopemeerkat-live-streaming-floyd-mayweather-mannypacquiao/32295201/>
31. Kosoff, M. 2016. 60 teenagers reveal what they think is cool — and what isn't — in 2016. Retrieved Feb. 17, 2016 from
<http://www.businessinsider.com/what-teens-are-like-in2016-2016-1>
32. Lavrusik, V. 2015. Introducing Live Video and Collages. Retrieved Feb. 17, 2016 from
<https://newsroom.fb.com/news/2015/12/introducing-live-video-and-collages/>

33. LeSure, M. 2015. Adding Live Streaming Apps to Your E-Resource Arsenal. *Journal of Electronic Resources Librarianship* 27.3: 199-201.
34. Li, S. 2015. A New Kind of Internet Pirate. Retrieved Feb. 17, 2016 from <http://www.theatlantic.com/technology/archive/2015/04/whats-stopping-people-from-periscoping-copyrightedmaterial/389228/>
35. McDonald, A.M., and Cranor, L.F. 2008. The cost of reading privacy policies. *ISJLP* 4: 543.
36. Morrison, K. 2015. Beyond Periscope and Meerkat: The State of Live-Streaming Video. Retrieved Feb. 17, 2016 from <http://www.adweek.com/socialtimes/beyond-periscopeand-meerkat-the-state-of-live-streaming-video/620195>
37. Nilsson, M. 2015. Does The Periscope App Infringe Copyright? Retrieved Feb. 17, 2016 from <http://www.law360.com/articles/655708/does-theperiscope-app-infringe-copyright>
38. Perrin, A. 2015. Social Media Usage: 2005-2015. Retrieved Feb. 17, 2016 from <http://www.pewinternet.org/2015/10/08/socialnetworking-usage-2005-2015/>
39. Rainie, L. and Duggan, M. 2016. Privacy and Information Sharing. Retrieved Feb. 17, 2016 from <http://www.pewinternet.org/2016/01/14/privacy-andinformation-sharing/>
40. Reardon, M. 2016. Tech privacy policies need an overhaul, regulators say. Retrieved Feb. 17, 2016 from <http://www.cnet.com/news/tech-privacy-policies-needan-overhaul-regulators-say/>
41. Right of Publicity. 2016. Lumen database, Berkman Center for Internet & Society at Harvard University. Retrieved Feb. 17, 2016 from <https://lumendatabase.org/topics/31>
42. Right to Be Forgotten (EU). 2016. Lumen database, Berkman Center for Internet & Society at Harvard University. Retrieved Feb. 17, 2016 from <https://lumendatabase.org/topics/34>
43. Scholtz, J., and Consolvo, S. 2004. Toward a framework for evaluating ubiquitous computing applications. *Pervasive Computing*, IEEE 3.2: 82-88.
44. Solove, D.J. 2012. Introduction: Privacy self management and the consent dilemma. *Harv. L. Rev.* 126: 1880.
45. Shaw, T.J. Esq., ed. 2011. *Information Security And Privacy: A Practical Guide for Global Executives, Lawyers and Technologists*. American Bar Association (ABA), Chicago, IL, USA.
46. Terms of Service: Didn't Read. Retrieved Feb. 17, 2016 from <https://tosdr.org/>
47. Tyson, G., et al. 2013. Demystifying porn 2.0: A look into a major adult video streaming website. In *Proceedings of the 2013 conference on Internet measurement (IMC '13)*, 417-426. <http://dx.doi.org/10.1145/2504730.2504739>
48. Wee, A. 2015. Meerkat – Livestream available via Facebook. Retrieved Feb. 17, 2016 from <http://en.zinggadget.com/meerkat-livestream-availablevia-facebook/>
49. Williams, R. 2015. What is Twitter's new Periscope app? Retrieved Feb. 17, 2016 from <http://www.telegraph.co.uk/technology/2015/12/01/0/wh-at-is-twitthers-new-periscope-app/>
50. The Zettabyte Era: Trends and Analysis. 2015. Cisco Visual Networking Index initiative white paper. Retrieved Feb. 17, 2016 from http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-indexvni/VNI_Hyperconnectivity_WP.pdf
51. Zhang, L., et al. 2015. Kaleido: You Can Watch It But Cannot Record It. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom '15)*, 372-385. <http://dx.doi.org/10.1145/2789168.2790106>

52. Zimmer, M. 2005. Surveillance, privacy and the ethics of vehicle safety communication technologies. *Ethics and Information Technology* 7.4: 201-210.