Panel: Privacy Protection in Online Multimedia

Yung-Hsiang Lu
Purdue University
yunglu@purdue.edu

Andrea Cavallaro
Queen Mary University of London
a.cavallaro@qmul.ac.uk

Catherine Crump
University of California Berkeley
ccrump@law.berkeley.edu

Gerald Friedland
University of California Berkeley
fractor@icsi.berkeley.edu

Keith Winstein
Stanford University
keithw@cs.stanford.edu

ABSTRACT

Online multimedia has been growing rapidly due to ubiquitous mobile phones, widely deployed surveillance cameras, dashcams and mini-drones. When one takes photographs or videos at a public location, it is highly likely that some other people ("bystanders") also appear in the visual data. The data may be available online, such as shared by social media, and questions about privacy arise. This panel discusses the issues about privacy in online multimedia from legal, technological, and social aspects.

CCS CONCEPTS

• **Security and Privacy** → Social Network Security and Privacy;

• **Information Systems** → Multimedia Content Creation

KEYWORDS

Multimedia, Privacy, Legal

1 INTRODUCTION

Nearly three billion people have smartphones [1]; each phone has one or more cameras. Several hundred millions of surveillance cameras have been deployed [2]. Millions of vehicles are equipped with dashcams. Wearable cameras as well as cameras mounted on drones are increasingly popular. These cameras can capture visual data (image or video) almost anywhere at anytime. It is common that an unfolding event is captured by eye witnesses' mobile phones. Moreover, the visual data may be posted online and shared with friends or the general public. The data may include people (especially under-age minors) that are bystanders and thus raise questions about privacy of online multimedia.

Privacy issues have many aspects, including social, legal, and technological. This panel will discuss these different aspects of privacy.

MM'17, October 23-27, 2017, Mountain View, CA, USA.

ACM ISBN 978-1-4503-4906-2/17/10.
https://doi.org/10.1145/3123266.3133335

This paper examines sources of online multimedia, discuss legal aspects about the rights of acquiring, distributing, and consuming the data, possible unintended consequences of data sharing, as well as technologies that may be adopted to protect privacy.

2 ONLINE MULTIMEDIA

The first network camera was, perhaps, installed at the University of Cambridge for watching a coffee pot [3]. Since then, digital cameras are widely available and acquiring digital visual data as images or videos. Moreover, many social media sites offer unlimited free storage for posting visual data. About two billion images are posted on social media per day [4]; more than 400 hours of video are uploaded to Youtube per minute [5].

Online multimedia serves the purposes of sharing precious moments with friends and watching unfolding events. Meanwhile, the visual data (possibly also with sound) can raise serious questions about privacy.

In addition to social media, many governments deploy traffic cameras and make the visual data available to the general public. Transportation officials can obtain real-time information about congestion. Many organizations use cameras watching construction sites; some of them make the data available on the Internet. National parks, zoos, museums, and TV stations deploy network cameras providing video streams of tourist attractions. In most cases, only visual data is available; some cameras also capture sound and make it available on the Internet.

3 LEGAL ASPECTS OF PRIVACY FOR ONLINE MULTIMEDIA

One legal question that arises is whether individuals captured in video recordings have legal rights that constrain how footage of them can be used. This is primarily an issue when individuals are recorded in public places without first giving affirmative consent.

Because the U.S. is a common law system in which case law refines the contours of people's rights over time, the answer to this question is not entirely clear. However, it is fair to say that individuals' rights to control whether they are recorded in public places are quite limited, and restrictions tend to arise in narrow

and extreme cases. In the vast majority of circumstances, individuals are free to photograph others located in public places.

The U.S. is a federal system and there are many potential sources of law that could regulate capturing images. The federal government, state governments, and local governments all have at least theoretical power to regulate recording--if not to ban it then to place conditions on when and how it can be done. This alone means there is no one answer to the question of whether a recording implicates the legal rights of a person whose image is captured. That will depend on where the recording takes place.

Some legal rights only apply when the person doing the recording is a government actor (e.g. a police officer). For example, the Fourth Amendment to the U.S. Constitution protects against "unreasonable searches" and some video surveillance may be considered a search. However, the Fourth Amendment only restricts what the government can do. It does not apply when, for example, one private person records the activities of another private person in a public space.

In general, government recording will not run afoul of the Fourth Amendment absent special circumstances. Recording that is particularly lengthy (e.g. days not hours) or recording that captures the interior of a private space (e.g. a home) even when done from a public place may be treated as an exceptional case in which privacy protections are justified.

Conversely, the First Amendment to the U.S. constitution provides protections for free speech, and this protection has been construed to confer a First Amendment right to record activities in public places. This could prove a substantial obstacle to government attempts to regulate video recording, although there have been few cases on point so far.

Putting aside federal constitutional law, another question is whether any governments have passed laws restricting taking footage in public places. The general answer is no, although some have placed restrictions on certain narrow types of recording (e.g. "video voyeurism") or recording using certain means (e.g. drones).

Further, courts have also developed what are known as the privacy torts. This special body of law, developed by courts over time, protects private individuals against invasions of privacy by others. This body of law has been used by photo subjects to recover money damages against, e.g. paparazzi, but again only in extreme circumstances.

Assuming the footage is taken in compliance with the law, then those who acquire the footage are generally free to use it as they see fit subject to generally applicable laws (e.g. copyright law, contract law).

4 ONLINE PRIVACY VS OFFLINE PRIVACY

It is all too easy to think of the Internet as a separate world, and to assume one's online identities, actions, and relationships are somehow walled off from the "real-world" selves. This illusion of separation is created by the specialized, individually-operated technology we use to access the Internet [6]. In fact, one cannot even avoid the online "world" by not using online services; other people, companies, and organization can and will still share information about individuals.

Once information is shared online, it becomes part of what others know or can find out about individuals — and people do not have a strict dividing line in their minds between information they get from the Internet and any other type of information. In other words, someone's information footprint is not only the information in digital form; it encompasses everything that every other person, entity, or database knows about the person.

The online activities that are becoming an ever more integral part of everyday lives and identities can therefore be used by others to make decisions about us. For example, many employers, and even some colleges, will review a potential employee or student's social-media content before hiring or accepting them — and many people use the same method to check out a potential date.

Connection between contexts is not unique to the Internet; similarly, people's school or work lives are connected to their social lives. People may be judged in one context for how they behave in the other. However, the way information persists and is replicated on the Internet adds a new dimension.

5 TECHNOLOGY SOLUTIONS FOR PRIVACY PROTECTION

Protecting privacy in images and videos has been mainly related to concealing the identity of faces, whose location in the visual data can be defined manually or with a face detection algorithm. The identity is then hidden by redacting the region where the face appears or by replacing its pixel values with those of a de-identified face rendition that removes personally identifiable information.

Examples of de-identified renditions include avatars and statistically de-identified faces. Face de-identification algorithms may also use the k-anonymity property to make the identity of a person indistinguishable from that of k-1 (or more) other individuals by replacing a face with an average face.

Alternatively, the image region can be modified using pixelation, blurring or cartooning effects on the pixel values. An important objective to achieve here is to maintain the utility or aesthetic value of an image or video by introducing only a minimal distortion on the image content.

Privacy-preserving solutions for protecting faces also include scrambling and encryption to conceal a region of interest that is protected using a private key that can be used to recover the original data.

Irrespectively of the filter used to conceal personally identifiable information, the effectiveness of redaction and de-identified technologies mostly depend on the accuracy and

robustness of object detectors, which may fail under challenging pose or illumination conditions, as well as occlusions.

Moreover, gender, race, body shape and age information extracted from images can in turn leak personally identifiable information. Similarly, re-identification technologies that use clothing information and other soft-biometrics or contextual information such as location and objects may reveal the identity of an individual.

6 THE "RIGHT TO EAVESDROP" WHAT OUR OWN THINGS ARE SAYING ABOUT US[1]

Consumer devices today increasingly record audio and video and send it back to the manufacturer. Baby monitors, Nest cameras, smartphones, Alexa devices, and video-game consoles all do this.

This is part of a big battle, about the power and perils of Big Data and the cloud: Do the makers of these products really need the ability to collect data from the households of all the device owners and hold on to it? Voice, video, everything I ever put in my fridge, everywhere I've been — you can learn a lot about me from recording all that and saving it forever. Something I said in my TV's presence in 2017 could be used against me in 2037.

Today, though, I want to focus on a smaller question: how do we even figure out what is being collected about us?

There is no reliable way for consumer advocates to determine this for themselves. For example, Amazon states that its Alexa devices listen to audio all the time, but only transmit recordings that are made while the light is on (and shortly before the light turned on). Is this statement true? Can it be independently verified, and monitored, as the software on these devices is updated over time? The answer at present is no: Alexa talks to Amazon over an encrypted connection that even the device's owner cannot descramble.

To address this, my colleagues and I have proposed a "right to eavesdrop on your own things." We believe consumers--and consumer watchdogs--should have the ability to descramble the communications between consumer devices that they own and the cloud services those devices talk to. This would allow watchdog organizations (e.g., Consumer Reports, Underwriters Laboratories, or any interested busybody) to verify manufacturer's claims and discover when devices are collecting more than they should.

Just as you might not let your small child use the Internet unsupervised (and many parents instruct their children not to share their last name or address with the Internet), consumers should not be expected to allow their own devices, recording video or audio inside their homes, to have communications over the Internet that remain absolutely confidential from their owners.

I'll discuss this principle, the technical means by which it might be achieved, and some of the discussions we've had with makers of multimedia consumer devices and standards bodies.

7 CONCLUSION

Technologies have made it possible to acquire vast amounts of multimedia data and make it available online. Many important questions about privacy arise, including:

- Do people care about privacy? When? Where? Are there differences in age groups, cultures, education, geographical locations, time of day?
- Who has the rights to acquire the data (in particular, in public locations)? What are the restrictions of the rights?
- Who has the rights to view the data?
- Who has the rights to keep the data? How long can the data be kept?
- What are the social, economic, legal, and commercial values (or barriers) to protect privacy?
- How to protect against unauthorized access to data?
- What analyses can be performed on the data?
- What are the rights of the people that appear in the data?
- What technologies can protect privacy? Are the technologies ready? What are the costs of using these technologies?
- Can money be made by protecting (or violating) privacy? How? Who can benefit? Who loses?
- Should users set their own privacy rules? Or privacy should be protected by law?

REFERENCES

[1] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
[2] https://technology.ihs.com/532501/245-million-video-surveillance-cameras-installed-globally-in-2014
[3] http://www.bbc.com/news/technology-20439301
[4] http://www.businessinsider.com/were-now-posting-a-staggering-18-billion-photos-to-social-media-every-day-2014-5
[5] https://www.statista.com/topics/2019/youtube/
[6] http://www.teachingprivacy.org/
[7] http://www.politico.com/agenda/story/2015/06/internet-of-things-privacy-concerns-000107
[8] https://nsr.cse.buffalo.edu/mobisys_2017/papers/pdfs/mobisys17-paper32.pdf

[1]Includes excerpts from references [7] and [8].