6-9-2017

Bystanders' Privacy

Alfredo J. Perez

Sherali Zeadally

Scott Griffith

Bystanders' Privacy

Alfredo J. Perez, *Columbus State University*
Sherali Zeadally, *University of Kentucky*
Scott Griffith, *Columbus State University*

The widespread adoption of systems that collect ubiquitous sensor data from people using devices such as mobile phones, wearables, drones, and Internet-connected devices presents significant privacy challenges. Among these challenges is bystanders' privacy—that is, how to protect the privacy of third parties who could be affected when a sensing device is used in their surroundings.[1] By- standers' privacy arises when a de- vice that collects sensor data (such as photos, sound, or video) can be used to identify third parties when they have not given consent to be part of the collection.

It is not difficult to find examples in which bystanders were identified in photos taken by strangers, especially with the ubiquity of camera- enabled smartphones (there are more than 3.9 billion smartphones in the world, according to a recent Ericsson report; www.ericsson. com/mobility-report) and the avail- ability of identifying information on social networks and the Inter- net. A recent *Business Insider* news report describes a photographer's experiment of taking smartphone photos of bystanders at a subway station.[2] He identified people in the photos through free software, and bystanders identified in this experiment learned of their identification through news reports. Examples like this one have brought bystanders' privacy to the fore, even though this issue has been a longstanding challenge.

Human Aspects

Privacy in mobile, wearable, and connected devices usually focuses on either attacks and solutions that protect a user's private space from unauthorized access, or the protection of private data on social net- working sites and other services. With bystanders' privacy, however, there is a social aspect that extends the user's private space: when photos, videos, and sound are collected in shared or public spaces, a

conflict of space ownership arises between the user and bystanders. Using devices that can collect identifiable data creates the perception of ownership of the space surrounding the device (by device users), which can encroach on the space surrounding bystanders.[3]

The issue of bystanders' privacy is not new. Its origins can be traced to the invention of consumer- oriented cameras in the late 19th century. However, over the past few decades, this issue has risen in importance because of the ubiquity of mobile and wearable Internet- connected devices, and the proliferation of social networks that allow photos to be instantly shared with the world instead of secluded in a physical album (as was the case only a few decades ago).

In the early 2000s, research on human-computer interaction found that cellphone use in public spaces was offensive to some people;[4] these devices presented a conflict of social spaces in which a user was simultaneously in the physical space that he or she occupied and the virtual space of the cellphone conversation. To- day, wearable devices such as smart glasses also include cameras and microphones that engender strong privacy concerns by collecting and sharing data over the Internet without permission, thereby directly threatening bystanders' space and autonomy.[5] Table 1 outlines and explains bystanders' fears and concerns in greater detail.

Table 1. Bystanders; privacy concerns.[5]

Privacy concern	**Description**
Facial recognition	Association and recognition of a bystander with a place or a situation in which the bystander would not wish to be recognized by others
Social implication	Lack of awareness by a network of friends regarding data being collected about them
Social media sync	Immediate publishing or sharing without the bystander's knowledge
User fears: Surveillance and sousveillance	Continuous tracking of activities that might make a user or bystander feel that no matter what he or she does, everything is recorded
Speech disclosure	Capturing speech that a user or bystanders would not want to record or share
Surreptitious A/V recording	Recording audio or video that might affect bystanders without their permission
Location disclosure	Fear of inadvertently sharing a location to third parties that should not have access to the location information

Does the general public care about bystanders' privacy? Results from a recent survey that explored users' preferences when photo- graphed as bystanders showed that more than 95 percent of responders answered positively to this question.[6] This survey also showed trends that indicated responders were more aware and re- strictive about being photographed as bystanders. These trends were in venues such as beaches, gyms, and hospitals; with strangers in social situations; and when images are shared online.[6]

Current Solutions

No current technological method has been widely adopted to protect bystanders' privacy because many solutions exist only as prototype systems in the research stage (an exception is recording devices with LEDs that notify users and bystanders that data collection is being performed in their surroundings, but not all smartphones and wearables have this feature). How- ever, the utilization of privacy- enhancing wearables could become popular because these devices give bystanders the choice of protecting their own privacy rather than trusting their protection to others, potentially creating a market for these devices.

The techniques proposed to protect bystanders' privacy fit into two major categories: location-de- pendent methods, which deny user devices the opportunity to collect data; and obfuscation-dependent methods, which prevent by- standers' identification. Figure 1 presents the taxonomy we use in this section to classify the methods available to protect bystanders' privacy.

Location-Dependent Methods

The goal of location-dependent methods is to deny the collection of data in particular shared spaces (such as restaurants, casinos, or cafes). The implementation of this method usually entails restricting and banning devices' use through warning signs, confiscating de- vices before users enter a shared space, or temporarily disabling devices in the shared space.

According to Jeff Jarvis's book *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live* (Simon & Schuster, 2011), President Theodore Roosevelt banned the use of cameras at public monuments in Washington, DC, around

1903, and they were often banned at beach- es as well. Similar bans occurred in England during World War I. In the US, using cameras and recording devices to collect data about things that are plainly visible in public spaces is now treated as a constitutional right. For example, the ruling in Glik v. Cunniffe established a precedent in which citizens have a right to film police officers under the First Amendment in public spaces un- der certain reasonable limitations of time, place, and manner.[7]

Devices can be disabled in shared spaces using three approaches: sensor saturation, broadcasting commands, and context-based approaches. With sensor saturation, the goal is to make sensors in user devices sense an input signal that is greater than the maximum possible measurable input those sensors support (thereby making them unusable by saturation). This saturating signal is broadcast by fixed devices in shared spaces. By- standers' privacy is protected be- cause when users' device sensors are saturated, they will report data which do not provide or reveal any usable information to identify by- standers. An example in this category includes using near-infrared pulsating lights from fixed devices in shared spaces and directing them at the mobile device's cam- era lens[8] to saturate the charge- coupled device (CCD) sensor. This near-infrared light is invisible to the human eye, but causes the CCD sensors to saturate. This system was implemented as a proof- of-concept, and no consumer version of this prototype exists on the market.

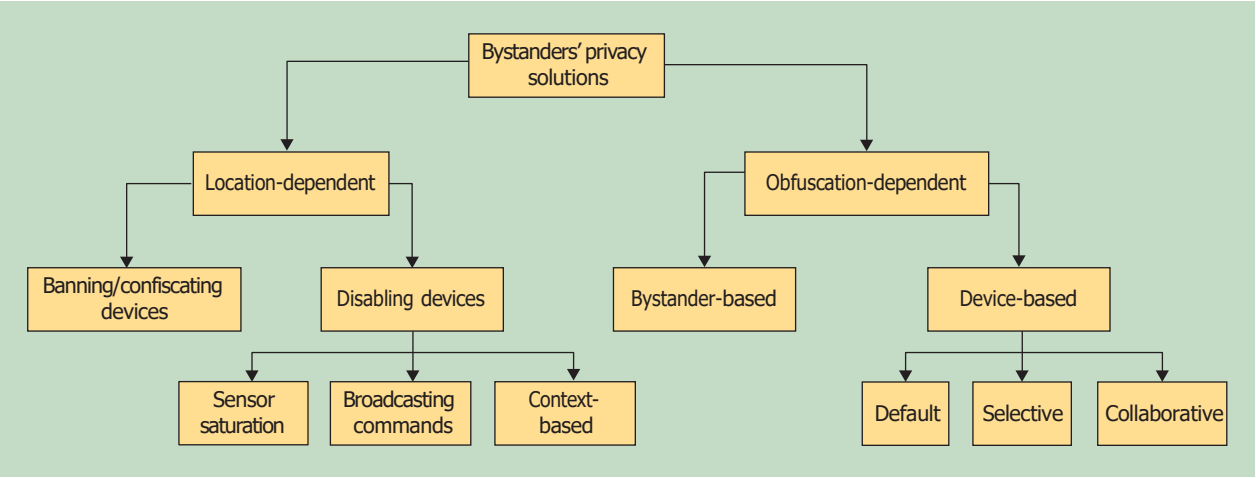

Figure 1. Taxonomy of methods for bystanders' privacy protection.

Broadcasting commands to temporarily deny user devices the chance to collect data in shared spaces can protect bystanders' privacy. The goal in this category is to use communication protocols combined with fixed devices (for example, access points) to broad- cast commands that cause the user's device software to disable the user device's sensors. Examples in this category include Bluetooth- based protocols and infrared light-based protocols that can be used to send commands from fixed devices in shared spaces to disable users' device sensors.[9] Bystanders' privacy is protected because data cannot be collected by user devices when these disabling commands are broadcast.

Apple patented the use of infrared communication protocols to send disable commands for cell- phones,[9] but no reports on public utilization or the availability of this technology exist. In the case of Bluetooth-based protocols that can disable sensors, no consumer product has implemented this technology.

In the final category (context- based approaches), user devices perform some type of context recognition to trigger software actions that will deny explicit data collection by disabling device sensors in shared spaces. An ex- ample in this category includes the virtual walls approach,[10] in which the device uses contextual information (such as GPS location data) to trigger software actions that can temporarily disable its sensors based on preprogrammed contextual rules. In this case, by- standers' privacy is preserved because data cannot be collected by user devices when the user's con- text is recognized and the device's sensors are disabled. No commercial product currently implements context-based sensor-disabling mechanisms.

Obfuscation-Dependent Methods

Obfuscation methods attempt to hide bystanders' identity to avoid their identification. These methods can be classified in two groups: bystander-based obfuscation and device-based obfuscation.

In bystander-based obfuscation, bystanders take action to avoid identification. This might be accomplished by wearing some type of hardware (or clothing) that hides or perturbs the identifiable features (such as facial features) needed to perform identification.[11,12] Or, by- standers might perform some type of physical action (for

example, leaving the shared space or asking a user to stop using a device) to protect their privacy when they become aware of a device's use in their surroundings that might in- fringe upon their privacy.[1]

Privacy Visor wearable glasses[11] are an example of a device that performs bystander-based obfuscation. Worn by bystanders, these glasses use near-infrared light to block those facial features required by image-processing algorithms to perform facial recognition. Typical facial-recognition algorithms detect the difference in contrast between eyes and cheeks (the eye region is darker than the cheek region). By using near-infrared light (invisible to the human eye) emitted by LEDs to illuminate the nose region be- tween the eyes, this wearable causes an effect on CCD sensors in cameras similar to saturation. The result diminishes the contrast that detects the difference between regions in a face, thereby preventing algorithms from detecting the bystander's face.

A second example includes the use of perturbed eyeglass frames, which a bystander could use to impersonate other individuals' facial features or to deceive facial-recognition and identification algorithms.[12] These eyeglass frames have a physical distribution of colors on their surface that adds noise to the captured data in such a way that the algorithms either misclassify the bystander's face as another individual (impersonation), or are confused so that they do not detect a face. This technology was recently developed as a research project to undermine facial identification algorithms; no current commercial product exploits this idea yet.

Notification methods that alert bystanders to protect their privacy include the use of LEDs on wearables to notify bystanders of video or audio being recorded in their surroundings (such as Snap spectacles), and the use of short-range radio broadcasts and Wi-Fi-based communication protocols to notify bystanders about sensing activity being performed in their proximity (such as the NotiSense system[1]).

In the device-based obfuscation category, the software on users' devices adds noise (such as blur- ring) on collected data to hide by- standers' identifiable features (such as facial features or voice features, in cases of sound collection). Such software might perform obfuscation by default (for example, blur- ring all faces detected in a photo or video), might let users add noise to obfuscate bystanders selectively (selective

obfuscation), or might access protocols over wireless networks to communicate bystanders' privacy settings such that the software on the user's device could automatically hide bystanders' identifiable features based on these settings (collaborative obfuscation).[6] The drawback of device-based obfuscation is that these methods rely on devices controlled by the user, not the bystander.

Open Issues

Many of the methods we de- scribed are still being explored in research projects and have not been exploited commercially. Thus, the development of new products that incorporate features designed to protect bystanders' privacy remains an open challenge and opportunity. Manufacturers can leverage the Privacy by Design framework to incorporate algorithms for blurring or protocols to disable cameras or notify bystanders' smartphones, wearables, and other devices.

Recent advances in deep learning combined with image processing can recreate images that were blurred by obfuscation methods, thereby weakening the effectiveness of some methods intended to protect bystanders' privacy. One good example is the pixel-recursive super- resolution method, which trans- forms low-resolution images with blurred faces into high-resolution images with the original facial features recovered. A possible solution for managing reidentification can be achieved by substituting by-standers' faces with fake, computer- generated faces, or faces taken from public-domain photos to obfuscate real images obtained of bystanders. Other methods, such as gait-identification techniques, or methods that use unique identifiers broadcast by mobile phones and wearables (that is, MAC addresses from network interfaces) could also be used to reidentify bystanders. More research is needed to protect bystanders from such techniques.

Finally, social acceptance of technology because of its benefits has fueled the adoption of many devices despite their drawbacks. It has been argued that this will be the case with devices that could potentially violate bystanders' privacy. Nevertheless, the Google Glass scenario seems to tell another story: in May 2013, Google issued a statement saying that applications that incorporated facial recognition in their Google Glass Explorer Program would not be accepted into the program because of strong

public concerns. Indeed, recently, many news outlets have pointed to Google Glass privacy concerns as one reason for its demise. It re- mains an open issue how, in the future, the public will adopt and use devices that could violate both user privacy and that of bystanders.

As new, more powerful Internet-connected and sensor-enabled devices emerge (especially in the mobile and wearable market), it becomes easier to collect identifiable data about bystanders. As this trend continues, the issue of protecting bystanders' privacy will come into even greater focus. We analyzed current solutions addressing this issue, but a great deal of work is needed to solve the outstanding issues we outlined.

Acknowledgments

Alfredo J. Perez was supported by the US National Science Foundation under award 1560214. Sherali Zeadally's work was support- ed by a University Research Professorship Award from the University of Kentucky in 2016.

References

1. S. Pidcock et al., "Notisense: An Urban Sensing Notification System to Improve Bystander Privacy," *Proc. 2nd Int'l Workshop Sensing Applications on Mobile Phones*, 2011, pp. 1–5.
2. A. Heath, "This Russian Technology Can Identify You with Just a Picture of Your Face," *Business Insider*, 22 June 2016; read.bi/2p83hOU.
3. R. Mitchell, "Sensing Mine, Yours, Theirs, and Ours: Interpersonal Ubiquitous Interactions," *Proc. 2015 ACM Int'l Symp. Wearable Computers*, 2015, pp. 933–938.
4. L. Palen et al., "Going Wireless: Behavior & Practice of New Mo- bile Phone Users," *Proc. ACM Conf. Computer Supported Cooperative Work*, 2000, pp. 201–210.
5. V.G. Motti et al., "Users' Privacy Concerns about Wearables: Impact of Form Factor, Sensors and Type of Data Collected," *Proc. 1st Workshop Wearable Security and Privacy*, LNCS 8976, 2015.
6. P. Aditya et al., "I-Pic: A Platform for Privacy-Compliant Image Capture," *Proc. 14th Ann. Int'l Conf. Mo- bile Systems, Applications, and Services*, 2016, pp. 249–261.

7. Glik v. Cunniffe, *Federal Reporter*, 3rd series, vol. 655, 2011, p. 78 (US Court of Appeals for the First Circuit).
8. K.N. Truong et al., “Preventing Camera Recording by Designing a Capture-Resistant Environment,” *Proc. Int’l Conf. Ubiquitous Computing*, 2005, pp. 73–86.
9. V. Tiscareno, K. Johnson, and C. Lawrence, *Systems and Methods for Receiving Infrared Data with a Camera Designed to Detect Images based on Visible Light*, US patent 8,848,059, to Apple, Patent and Trademark Office, 2014.
10. A. Kapadia et al., “Virtual Walls: Protecting Digital Privacy in Pervasive Environments,” *Proc. Int’l Conf Pervasive Computing*, LNCS 4480, 2007, pp. 162–179.
11. T. Yamada et al., “Use of Invisible Noise Signals to Prevent Privacy Invasion through Face Recognition from Camera Images,” *ACM Multi- media*, 2012, pp. 1315–1316.
12. M. Sharif et al., “Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition,” *Proc. ACM SIGSAC Conf. Computer and Communications Security*, 2016, pp. 1528–1540.

Alfredo J. Perez *is an assistant professor with the TSYS School of Computer Science at Columbus State University. Contact him at perez_alfredo@columbusstate.edu.*

Sherali Zeadally *is an associate professor in the College of Communication and Information at the University of Kentucky. Contact him at szeadally@uky.edu.*

Scott Griffith *is a graduate assistant with the TSYS School of Computer Science at Columbus State University. Contact him at griffith_scott@columbusstate.edu.*