BlindSpot: Creating Capture-Resistant Spaces

Shwetak N. Patel, Jay W. Summet and Khai N. Truong

Abstract The increasing presence of digital cameras and camera phones brings with it legitimate concerns of unwanted recording situations for many organizations and individuals. Although the confiscation of these devices from their owners can curb the capture of sensitive information, it is neither a practical nor desirable solution. In this chapter, we present the design of a system, called BlindSpot, which prevents the recording of still and moving images without requiring any cooperation on the part of the capturing device or its operator. Our solution involves a simple tracking system for locating any number of retro-reflective CCD or CMOS camera lenses around a protected area. The system then directs a pulsing light at the lens, distorting any imagery the camera records. Although the directed light interferes with the camera's operation, it can be designed to minimally impact the view of other humans in the environment. In addition to protecting one's personal or private space from unwanted recording, the BlindSpot system can be used to turn spaces, such as industry labs, movie theatres, and private properties, into capture-resistant environments.

1 Introduction

As digital cameras and camera phones have become cheaper and more common, it has also become easier for owners of these devices to record still and moving images anywhere. The pervasiveness of such recording devices creates a legitimate concern among those who wish to retain some level of privacy or secrecy. Companies concerned that camera phones may compromise the security of their intellectual property often ban such devices from their facilities. Although this approach and other legal and social forces may curb inappropriate capture behaviors [1, 3, 9], such practices are not always practical or reliable. Thus, there has been previous

S.N. Patel (✉)
Computer Science and Engineering and Electrical Engineering, University of Washington, Seattle, WA 98195, USA
e-mail: shwetak@cs.washington.edu

A. Senior (ed.), *Protecting Privacy in Video Surveillance*,
DOI 10.1007/978-1-84882-301-3_11,

work that addressed this challenge by disabling recording features in the cameras through cooperative software [5, 7, 10]. Alternatively, we explored a solution that does not require instrumentation or control of the recording device. We developed a system for safeguarding the environment itself against unwanted recording, called BlindSpot. The system allows people to prevent unwanted recording of their own personal space. Our system actively seeks cameras in the environment and emits a strong localized light beam at each device to neutralize it from capturing while minimally disturbing the natural viewing experience by the human eye.

In this chapter, we summarize some previous work in this area. We then outline the technical underpinnings of our approach, describe a prototype implementation of the BlindSpot system and discuss the advantages and limitations of this approach for safeguarding against digital capture. Finally, we discuss the potential application of the BlindSpot system in industry labs, movie theatres, and private properties to turn those spaces into capture-resistant environments.

2 Related Work

Most technical solutions previously proposed to prevent or react to undesired camera capture require some sort of instrumentation on the capture device. Solutions, such as Safe Haven, leverage the short-range wireless capability available on camera phones (such as Bluetooth or WiFi) to allow the environment to notify the device that the space does not allow photography or other forms of recording [5, 7, 10]. A drawback to this solution is that it requires the camera phone owner to install and use special software on her/his device and respect the privacy constraints of the environment and nearby individuals. For example, Hewlett-Packard's proposed paparazzi-proof camera [8] automatically modifies images when it receives commands from a remote device. This camera includes a facial recognition feature that selectively blurs parts of an image that include faces of particular people. Similarly, Cloak addresses privacy concerns with surveillance cameras by having users carry a "privacy enabling device" (PED) [2]. This device informs the environment that any footage of the carrier of this device must be sanitized later.

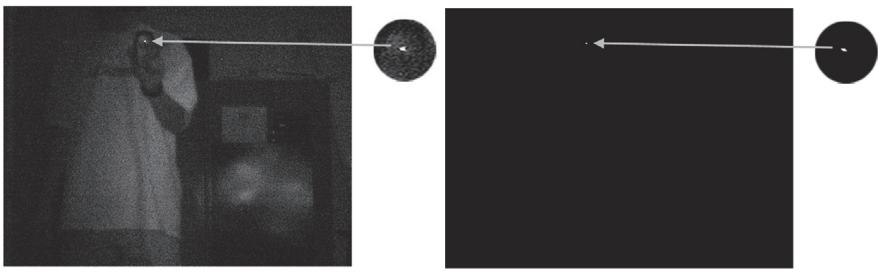
Alternatively, a small wearable solution called "Eagle Eye" uses a light sensor to detect a camera's light flash [4]. In response, this device instantaneously flashes back and obscures a portion of the photographic image. However, the device only works against still, flash photography.

We take a significantly different approach from these previous solutions in the design of Blindspot, which enables the definition and creation of capture-resistant environments. First, we actively impede recording at the point of capture, as with Eagle Eye, rather than requiring users to trust cameras to sanitize images after the recording has occurred. Second, unlike many previous solutions, our approach does not rely on any cooperation or instrumentation on the part of the capture devices or the people operating them. Our solution addresses both video capture and still imagery. We focus on being able to protect fixed regions within an environment, such as a wall. Specifically, our solution will minimally impact what an observer in the environment sees while still preventing a camera from being able to record. That

is, surfaces in an environment obviously can be covered to prevent capture, but then visitors to the space cannot see anything at all. Additionally, there are numerous commercially available retro-reflective sprays and shields that can also be placed over a surface to reflect light and flashes in a manner that prevents recording. However, these solutions create glare that impacts visibility from the human eye as well as the camera's CCD or CMOS sensor whereas our system does not affect people in the environment.

3 Design Goals for a Capture-Resistant Environment

Our primary goal in addressing this problem was to design a system that prevents certain portions of that space from being recorded with a standard CCD or CMOS camera, thereby producing a so-called capture-resistant environment. This motivation, and review of past related work, highlights the four major design goals for building a capture-resistant environment. First, the environment would not require cooperation or control of the recording devices before, during, or after capture. Second, it should be able to prevent both still images and video recordings. Third, the view of the environment by the naked human eye must be minimally impacted. Finally, we wanted our approach to allow authorized cameras to record. Using a combination of computer vision and projection, our design, described in the next section, actively searches for cameras and systematically blocks them from recording clear pictures, rather than relying on the cameras to remove or alter content after the fact (see Fig. 1).



(a) (b)

Fig. 1 On the *left* is an unprocessed IR view captured by our camera detector with plenty of ambient light in the room. A person holds a camera phone pointed at a region in the environment we want to protect from capture. On the *right* is the processed view. The camera is detected by locating a bright white circular speckle

4 The BlindSpot System

In this section, we present our BlindSpot system, which consists of three components. The first component – the camera detector – actively tracks CCD or CMOS lenses in the environment. When the system detects a camera lens, the second

system component – the camera neutralizer – sends a localized beam of light at each camera's lens to obstruct its view of the scene. This technique also works on video cameras. The third part of the system – the capture manager – regulates camera capture within the environment. This component locates and allows permitted devices to record. For each component, we describe the theory of operation and our proof of concept implementation. We then critically evaluate the limitations of our proof of concept prototype, distinguishing the theoretical limits from the current engineering limitations of the specific implementation. We also discuss future extensions of our system.

4.1 Detecting Cameras in the Environment

CCD and CMOS cameras have an optical property that produce well-defined light reflections. Our system tracks these reflections to locate cameras in the local environment.

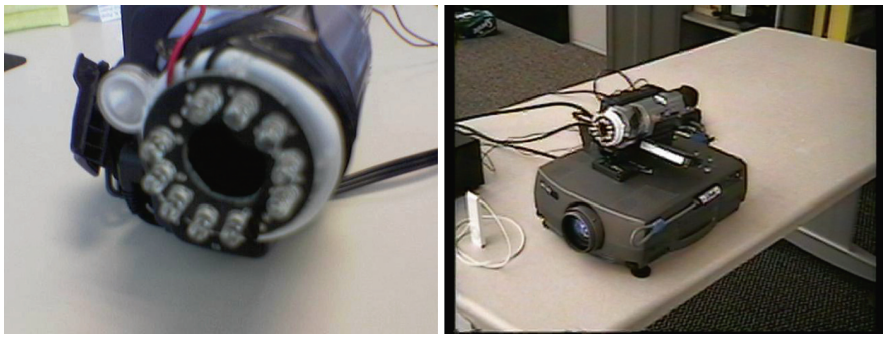
4.1.1 Theory of Operation

BlindSpot's camera detector leverages the retro-reflective property of the CCD or CMOS sensor lens found on all consumer-level digital cameras. Retro-reflection causes light to reflect directly back to its source, independent of its incident angle. CCD and CMOS sensors are mounted at the focal plane of the camera's optical lens, making them very effective retro-reflectors. By tracking these retro-reflections, we can detect and locate cameras pointed towards a given direction.

There are many objects in the environment that also exhibit the retro-reflective property. Commercial applications of retro-reflection include traffic signs and reflective clothes commonly worn by road construction workers. In addition, the retro-reflective property of the retina at the back of the eye often causes a subject's eyes to glow red in flash photography. This effect has allowed researchers to use a similar approach to ours to track eye movement in gaze tracking systems [6]. As we show later in this chapter, these objects are typically imperfect retro-reflectors and can reasonably be distinguished from CMOS or CCD cameras.

4.1.2 Implementation

In our initial prototype, we used a Sony Digital HandyCam video camera placed in *NightShot* mode to detect cameras in the environment. We arranged IR transmitters and covered the detector's lens with a narrow band pass IR filter (see Fig. 2). This instrumentation projected an IR light beam outwards from the camera and detected any retro-reflective surfaces within the field of view. We intentionally placed the IR illuminator around the perimeter of the detector's lens to ensure a bright retro-reflection from cameras within the field of view of the detector and pointed directly at it or tilted away at slight angles (which we computed to be up to roughly $\pm 20^{\circ}$ for our apparatus). Retro-reflections appeared as a bright white circular speckle through



(a) (b)

Fig. 2 The *left* picture shows our initial camera detector unit. We outfitted a Sony HandyCam, placed in *NightShot* mode, with a collection of IR transmitters and covered the lens with a narrow band pass IR filter. The *right* picture shows our camera detector coupled with a projector to neutralize cameras in the environment

the IR filtered camera. We initially thought that by flickering the IR light at 5 Hz, we would be able to detect reflective surfaces more easily. Although this approach worked, we later relied on computer vision techniques to detect the reflections and did not need to flicker the IR light.

We detect reflections by simply locating white regions in the camera view above a certain color threshold (in gray). The system disregards all other shades of gray, assuming these reflections come from some surface other than a lens. Because we employ thresholding technique, there is no limit to the number of devices that the camera detector can detect within its cross-section. In the next section, we discuss how to handle false positives and false negatives.

The system effectively tracks cameras and their trajectories at about 15 Hz. A more powerful computer could track at 30 Hz; however, 15 Hz is sufficient because a user must hold the average camera still for at least this period of time to avoid motion blur during capture. The detector camera has about a 45° field of view. We have found that reflections from cameras of varying shapes and sizes can be detected from up to 10 m away. At 5 m away, the cross-section of the detector camera is roughly a 4 m width × 3 m height area (see Fig. 3).

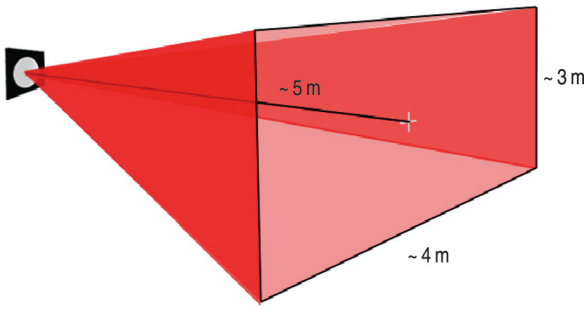


Fig. 3 At 5 m away, the cross-section of the detector camera is roughly a 4 m width × 3 m height area

Fig. 4 Current implementation of the BlindSpot system

Because the original implementation used a single camera, the system required manual calibration between the camera detector and the neutralizer (described in the next section) to a planar surface. To address this problem, we implemented the current prototype to use two webcams as a stereoscopic vision system for tracking in 3D space (see Fig. 4). This approach supports the flexible placement of the neutralizer and the camera detectors independent of each other.

4.2 Neutralizing Cameras

Once the system detects camera lenses in the environment, the camera neutralizer component emits localized light beams onto detected camera lenses. The strong beam of light forces the camera to take an obscured image.

4.2.1 Theory of Operation

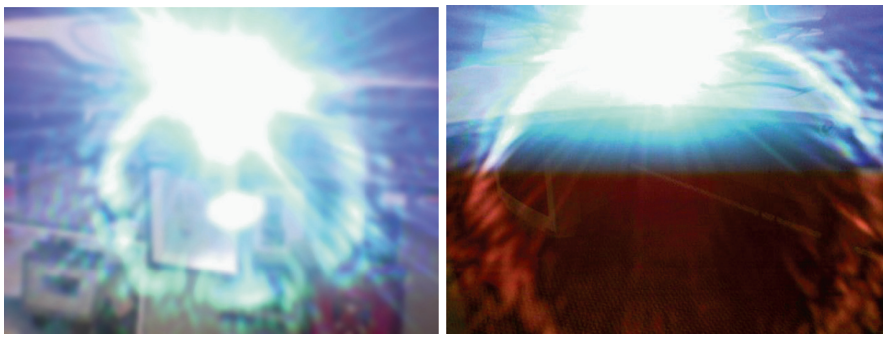
The camera neutralizer leverages the inherent imperfect sensing capabilities of CCD and CMOS cameras that result in two specific effects, blooming and lens flare. Blooming occurs when a portion of the camera's sensor is overloaded, resulting in leakage to neighboring regions. For example, a candle in an otherwise dark setting may cause blobs or comet tails around the flame. Although some cameras are capable of compensating for this effect, they typically only handle moderate amounts of light. Lens flare is caused by unwanted light bouncing around the glass and metal inside the camera. The size of the lens flare depends on the brightness of the entering light. Well-designed and coated optics can minimize, but not completely eliminate, lens flare. By shining a collimated beam of light at the camera lens, blooming and

lens flare significantly block any CCD or CMOS camera from capturing the intended image. Some cameras employ bright light compensation algorithms. However, there is typically a delay before the sensor stabilizes. Thus, a flashing light prevents the camera from stabilizing to the light source.

4.2.2 Implementation

To emit a strong localized light beam at cameras, we pair a projector of 1,500 lumens with our camera detector. This unit projects an image of (one or more) spots of varying light at the reflections. Pixels in the projected image change between white, red, blue, and green. This approach prevents cameras from adjusting to the light source and forces the cameras to take a picture flooded with light. In addition, interleaving various projection rates neutralizes a larger variety of cameras. The camera neutralizer continuously emits this light beam until the camera lens is no longer detected. Therefore, this approach works against both still image cameras and video cameras.

Our tests show that the projector can still generate an effective localized light beam when we focus it to 5 m away. Although light from a projector can travel much further, its luminance decreases with distance. We estimate that 5 m is roughly the length of a reasonable size for a room. At 5 m away, we can project localized light beams to cover a pyramidal region with a base of 6 m width $\times$ 4.5 m height. To ensure that we can neutralize cameras from all angles, we can measure the angle at which users can approach the surface, and accordingly, we can determine how many projectors we must use to cover that range. We can add additional projectors away from the surface to neutralize cameras from further away if needed (see Fig. 5).



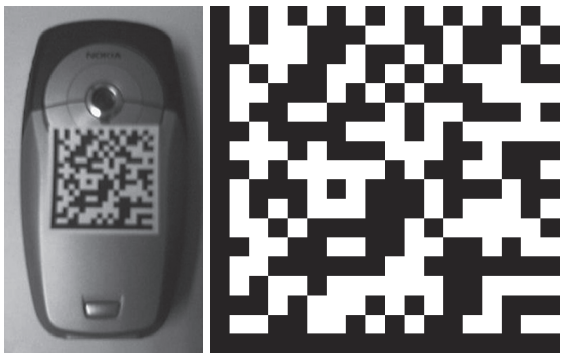
(a) (b)

Fig. 5 Images taken from a camera hit by localized light beam emitted by our camera neutralizer. The picture on the *left* shows a localized light beam generated using a single color. The picture on the *right* shows a localized light beam generated using color patterns that do not allow the cameras to adjust to the light source (notice the scan line)

4.3 Regulating Camera Capture

Although our system prevents existing cameras from being able to record a fixed surface in our environment, we recognize that there may be circumstances in which it would be appropriate for certain cameras to be permitted to capture. To allow certain cameras to take pictures in the environment, the system simply does not send localized light beams at those devices. However, this feature requires that the environment knows which cameras have been permitted by the owner of the space to take pictures.

One solution we implemented is placing a physical token on the lens side of the camera. The tag is retro-reflective and depicts a 2D glyph. When the camera detector finds this tag within close proximity (1–5 m) of a camera lens and the system validates its authenticity, the camera neutralizer is not activated for that particular camera. The 2D glyph encodes a unique identifier that the system recognizes as valid tags. The owner of the physical space gives out a tag when she wants to permit a specific camera to capture within that space. The owner either removes the tag after the camera has captured information or she removes the 2D glyph from the list of tags the capture-resistant environment permits. A problem with this solution exists when a camera lens is in the detector's field of view but the 2D glyph has been occluded. The glyph must be placed very close to the camera lens to address this problem. If spaced over some distance, our tracker may become confused between the permitted camera lens and another nearby lens (see Fig. 6).



(a) (b)

Fig. 6 *Left* shows retro-reflective glyph temporarily attached near a camera phone's lens. *Right* shows sample 5 cm × 5 cm glyph pattern

5 Assessing the Design Challenges and Limitations

In this section, we summarize how we addressed our original design goals and the challenges and limitations faced in the design of BlindSpot. We also describe how our approach addresses the potential attacks or workarounds people may use to

circumvent the capture-resistant environment. Finally, we also discuss the known theoretical limitations and the engineering deficiency in our prototype.

5.1 Challenges

There are two types of challenges our system faces. First, we must handle the errors involved in detecting cameras. Second, we must address potential attacks or workarounds people may use to circumvent the capture-resistant environment.

5.1.1 Errors in Detecting Cameras

There are two types of errors that can occur in our system. A false positive occurs when the camera detection system mistakenly detects a camera in the environment where one is not actually present. A false negative occurs when the camera detector fails to identify a camera pointing at the capture-resistant space.

Handling False Positives

False positives can result from the detection system interpreting reflections off of metallic or mirrored surfaces present in the space. Because these surfaces potentially produce the same reflective speckle as a CCD or CMOS sensor, the system would target a non-existent camera.

False positives are not detrimental to the operation of the system. However, the superfluous projector light produced by the false positive may be distracting or even bothersome for users in the environment. The worst false positive situation occurs when the system incorrectly identifies a region near a person's face as a potential camera, irritating or even harming the person's vision.

We address these problems by further analyzing the potential camera speckles. For the case of a reflection caused by metallic or other lens-like surfaces we can determine a false positive by inspecting the suspected reflection from multiple vantage points. The reflection caused by the CCD or CMOS camera has a consistent appearance off its surface. If the reflection moves at a different vantage point views, then it is not a camera-based reflection. These other surfaces are imperfect reflectors, which is typically attributed to the surface curvature, such as eyeglasses or imperfect finishes like brushed metal. To reduce the number of false positives, our system uses two cameras spaced apart and pointed at the same region to detect when a reflection moves in different vantage view points. Another strategy is to place multiple illuminators on the same plane as the detector and then cycle between each light source. Reflected light that is not coaxial to the detector's view indicates that the reflector is an imperfect retro-reflective surface or not retro-reflective at all. Because eyes have a similar retro-reflective signature to cameras, they are likely to cause the most false positives. However, unlike camera lenses and CCD sensors, the human eye is not a perfect retro-reflector and thus we can employ this strategy to help guard against incorrectly detecting eyes as cameras (Fig. 7 shows an example of using two off axis illuminators).

Fig. 7 Anti-piracy prototype of the BlindSpot system being set in a movie theatre setting. The camera detection device is placed near the movie screen facing the audience

Handling False Negatives

Unlike false positives, false negatives are detrimental to the security of the space. One solution is to take a naïve approach and assume that any reflection is a potential camera. This may be appropriate when security is of utmost importance. However, this approach does not work when the CCD camera does not produce a reflection. Occlusion of the CCD from the camera detector is the primary reason for this, but typically an occlusion of the CCD inherently blocks a photograph from being taken in the first place. The camera can be angled sufficiently enough away that the incident light fails to reach the detector camera. In this case, the camera is already turned far enough away such that the capture-resistant space does not appear in its field of view. Thus, if there is no light reflection from the CCD, then the CCD camera cannot see the region around the detector.

We can place multiple pairs of camera detectors around a space for added security. From our experience, we have found one pair to be sufficient. A cheaper alternative is to place multiple IR light emitters throughout the space to increase the likelihood for a reflection. This solution may increase the number of false positives; however, its cost effectiveness outweighs those concerns.

We did not implement dead reckoning, but this approach would address the momentary loss of camera lens tracked by the system. By observing the trajectory of the cameras, the neutralizer continues to project the beam at the inferred path in hope of hitting the camera. This scheme works for very short-lived blips lasting a few seconds. Anything longer would likely make the dead reckoning ineffective.

5.1.2 Attacks and Workarounds

Aside from physical vandalism to the capture resistant environment, we identify some workarounds users may employ with their CCD or CMOS camera. We discuss how our system design addresses some of these attacks, explaining the non-obvious reasons behind why these attacks would not work. Where appropriate, we provide some theoretical justification.

Masks and Filters

An attacker may try to mask the camera lens with surfaces such as a lens from a pair of sunglasses. Typical sunglasses do not block IR light, and thus BlindSpot would still detect the CCD or CMOS sensor lens. Mirrored and even polarized sunglasses also fail to prevent the camera detector from finding the CCD. However, sunglasses are effective at mitigating the effects of the neutralizer on the camera. Sunglasses drastically reduce the intensity of the projected light. Despite this reduction, we have found that the light pattern and intensity we used in our system is still effective at neutralizing cameras from capture. A more intense and collimated neutralizing beam, such as from a laser, would certainly solve this problem.
IR filters pose the greatest problems for our particular system. In our current solution, we use pure IR light (880 nm) for CCD sensor detection. An 880 nm notch IR filter could be placed in front of a camera; this prevents IR light from reaching the CCD sensor while still allowing other visible light to pass. Because this is the greatest attack on our system, we can design our implementation to detect also IR filters in the environment and treat them as suspicious cameras. An IR filter reflection looks very similar to CCD sensor reflection to our camera detector (the only difference is a larger speckle size), thus making it a straightforward task to detect IR filters and treat them as a camera. However, this solution will result in more false positives. Because IR filters allow visible light to penetrate, the camera neutralizer is not affected by this attack.

Mirrors

A user can avoid pointing a camera at the capture-resistant region by using a mirror and taking a picture of the reflection on the mirror. However, our experience indicates that the camera detector can still clearly spot the CCD sensor in the mirror and the camera can be effectively neutralized by aiming back at the mirror. An attacker could hide a camera behind a one-way mirror to prevent it from being detected. Similar to the sunglass situation, IR light can still be detected appearing behind

a one-way mirror, making it an ineffective attack. In addition, images taken from behind a one-way mirror tend to produce low quality images in the first place.

Modifying Camera Sample Rate

The camera could be pre-programmed to sample at the rate of the neutralizer pattern. We addressed this problem by interleaving random frequencies for each pixel in the neutralizing projection pattern. In this case, CCD or CMOS cameras would not be able to synchronize to the projected pattern and frequency because of its inability to sample each pixel at different rates. Although our solution does not implement this interleaving, it is a fairly straightforward extension to our system.

Another possible workaround is to evade the neutralizing beam by moving the camera faster than our detector tracks. There is a limit to how fast the camera can be moved when taking a picture because of motion blur. The 15 Hz tracking rate of our implementation is sufficient for all camera phones and most digital cameras. High-end cameras with extremely faster shutter speeds require faster tracking. Increasing the area of the neutralizing beam would address this problem because of the larger movement needed to move outside the beam of the light.

5.2 Limitations

Our current implementation is limited to indoor environments, although we have found success near widows and areas where there is significant amount of natural light. However, for settings such as an outdoor concert, this system would need to be modified extensively to accommodate for such a large distance.

This solution works well with traditional CCD and CMOS cameras, but may have problems with extremely high-end cameras that have very fast shutter speeds and frame rates such as SLR. Other capture technologies that do not employ CCD or CMOS sensors, such as thermal imaging, cannot be detected using our scheme. These cameras are still very hard to produce, and we do not expect to see such high-end components integrated into a mobile phone anytime soon. Although the quality and resolutions of camera phones will increase, they do not have a direct impact on the effectiveness of this system (our system performed well even on a 4 megapixel CCD digital camera). Capture technologies that do not employ CCD sensors, such as ordinary film cameras, cannot be detected nor neutralized by our system.

Most camera systems employ some type of optical system; by instrumenting the environment to locate any reflection from optical devices, it is possible to detect any camera, including SLRs and ordinary film cameras. However, this approach would increase the false positive rate.

The conical region of the camera detector poses a problem with “dead zones” close to the detector/neutralizer system. A “dead zone” exists a short distance in front of the protected surface, directly underneath the detector unit, and on the azimuth. A person standing in this dead zone will be able to take a picture, although the resulting

image will be very warped. Placement of a physical barrier could limit proximity of users to the protected region and the "dead zone." Installation of another neutralizer at a lower level or different angle could cover the "dead zones" inherent to elevation and azimuth concerns.

Our system consists of three significant elements: a camera, a DLP projector, and a PC, costing a total of approximately $2500 USD. However, an actual implementation would be significantly cheaper. Video cameras are fairly affordable and will decrease in price with time. The PC is easily replaceable by a very inexpensive microcontroller. The projector is the most expensive of the three elements. We used a projector because of the ease in projecting concentrated light at very specific regions. Typical DLP projectors are designed to produce high-quality images at high resolutions, have tuner components, and incorporate sophisticated optical components. Our projection region is very small and does not require the level of optical precision and resolution available in typical DLP projectors. We can imagine a projector designed specifically for our application that is significantly cheaper. An even cheaper alternative and proper solution is to replace the projector with a scanning laser (similar to those found in laser light shows). By spinning a mirror and pulsing a laser at different rates, we can produce the same effect as we are creating with the DLP projector. This is not only a much cheaper solution, but also a more effective solution than a diffuse projector beam. Therefore, it becomes more practical to place many of these systems throughout a space for increased coverage.

6 Applying BlindSpot to Create Capture-Resistant Environments

Our original motivation for the design of BlindSpot was to build a system that would thwart picture taking of certain critical areas (inside of spaces such as office environments, conferences, tradeshows, and galleries) without having to confiscate recording devices from their owners. Within our research lab space, we often hang many posters that we created to present our project ideas internally amongst one another. In our initial demonstration of the system, we used BlindSpot to prevent the recording of one of our research posters. The poster was placed on one side of an 8-foot wide hallway. Although it was possible to take pictures at an angle up to 45° from 15 feet away on either side, the resulting pictures were usually extremely warped images of the poster. We used 2 sets of cameras and projectors to act as camera detectors and neutralizers. We instrumented these detectors and neutralizers above the poster to continuously monitor and protect a 90° sweep directly in front of it. When the system detected a camera, it neutralized it using the projectors. Both these steps happened automatically in the background without any manual intervention. Obviously, our approach did not prevent people from looking at the poster. Only when a user requested the right to take a picture did the owner of the space need to interact with the system to allow grant permission.

In this section, we present some interesting application ideas presented to us by others who have approached us during our development of this system, as well as the challenge of balancing against the lawless applications of this approach. The ideas presented to us by other interested parties include preventing the recording of copyrighted movies in theatres, protecting against industrial espionage, and using it as a part of an anti-paparazzi system. In addition to these applications of BlindSpot, we imagine obvious illegitimate uses of this system that may arise and must be addressed.

6.1 Anti-Piracy: Preventing Illegal Video Recordings in Movie Theatres

According to the Motion Picture Association of America (MPAA), the USA is the largest consumer of home entertainment products in the world, with consumer spend eclipsing $22.2 billion USD in 2002. In 2004, the US motion picture industry losses exceeded $3 billion USD in potential worldwide revenue due to piracy. The MPAA views optical disk piracy as the greatest threat to the audiovisual market in the USA, and the majority of all pirated products found in the USA is mastered from illegal camcording at theatrical screenings. Though movie piracy is an international problem, MPAA has spearheaded the worldwide effort to fight piracy, successfully lobbying Congress to introduce legislation and assisting in worldwide manhunts in pursuit of pirates around the globe. A sign of the MPAA's lobbying success was seen in early September 2005 when the Bush administration created the first Coordinator for International Intellectual Property Enforcement to help fight piracy. Though these efforts have made significant progress, movie piracy due to camcording continues to increase as box office numbers decline.

Simply delaying the release of pirated movies by just a few days can prevent the lost of hundreds of millions of dollars in revenues. Currently, a blockbuster takes just a few hours on average to go from full screening to illegal distribution over the Internet. There are over 30,000 screens in the USA, and one can imagine the logistical nightmare of guarding all of those, especially when theatre owners do not want to spend the money for extra security guards.

A potential application of the BlindSpot system is to actively prevent the illegal recording of movies. By no means would the system replace the security staff, but it would serve as a notifier for potential illicit activities. The BlindSpot system would be installed near the screens and directed towards the audience. Multiple units would need to be installed to cover large theatres, such as those with stadium style seating. During our development of this application, we quickly encountered concerns over the stigma of the "neutralizer" from the general public. Although the system is designed not to interfere with the viewing experience, the idea of a light beam being directed at the audience is not appealing from a marketing point of view. This is a tricky balance that must be solved. On one hand, the movie industry does not want to lose the revenues through piracy, but at the same time they also do not

want to upset the people who are actually paying to watch the movie in theatres. A potential solution is to employ just the detection component, which would notify staff members of the seat with a clandestine camera. It would be the responsibility of the staff member to call the appropriate authorities to rectify the situation.

6.2 Preventing Industrial Espionage

By the last quarter of 2006, approximately 85% of mobile phones in Japan were camera phones; it is expected this number will saturate at 85–90% in 2006. By 2010, more than 95% of mobile phones shipped in the United States and Western Europe will have cameras. Camera phones, and related consumer technologies, make it extremely easy to capture still and moving images anywhere and anytime. Companies concerned that camera phones can compromise the security of their intellectual property often ban such devices from their facilities. However, banning is no longer desirable or nor practical, because of the growing number of such devices that people will likely have and their reliance on those devices. At the same time, any visitor or employee could be involved in a plot to compromise a company's trade secrets. Thus, industrial espionage, especially in the form of stealing company secrets is a growing concern, with claims that it causes billions of dollars of loss in intellectual property annually. Companies can install BlindSpot simply to detect cameras (as described in the previous section). Alternatively, the system also can be used to continuously monitor and protect areas of their buildings in a manner similar to our demonstrated application of the system within our own lab space.

6.3 Anti-Paparazzi: Preventing the Recording of People

With the increasing prevalence of consumer recording devices, there is a growing concern over unwanted recording of individuals in public and privates spaces. For example, gymnasium owners interested in protecting the privacy of their customers can install BlindSpot in locker rooms and bathrooms.

Interestingly, some of the early interest in this technology came from an anti-paparazzi firm in Hollywood interested in instrumenting celebrity homes and automobiles with BlindSpot. After the Princess Diana tragedy, there has been much interest in curtailing future problems with unsolicited photographers all trying to get their perfect shot of high-profile individuals. BlindSpot could play an instrumental role in helping to deter much of this activity, especially from the "stalkerazzi," who try to take candid pictures on private property.

It is important to recognize, however, that photographers imaginably will try to find counter measures. This could lead to a whole new set of problems, such as tampering or vandalism. The danger of employing this system must be considered, as counter measures could pose even more dangers than there are now for the people being recorded and the innocent bystanders.

6.4 Illegitimate Uses of BlindSpot as a Digital Cloak

We believe there is value in employing a technology like BlindSpot for the purposes of protecting one's privacy, especially during a time when recording devices have become so commonplace that everyone is likely to have one with them. With an almost impossible task of opting out of being recorded or confiscating every capture device from individuals who enter a private or semi-private space, an autonomous system can be employed to help against this growing concern. However, one major challenge that we faced while developing BlindSpot is the potential use of this system for illegitimate or illegal activities.

It will be years before BlindSpot can be miniaturized to a point where an individual could wear it as a digital clock. However, we can imagine legitimate concerns which arise from a wearable version of our camera detector and neutralizer which prevents the recording of individuals in public spaces. While intended to protect someone's privacy or a company's intellectual property, individuals also could use the system to hide or evade from security cameras when performing inappropriate activities, such as when robbing a bank.

With any technology, it is often difficult to prevent individuals from using it for illicit means. One way to curb the problem of this technology from getting into the wrong hands is to control it at the point of sale through a licensing scheme. Only authorized customers who can guarantee proper installation and security of the system itself would be allowed to purchase the system. In addition, areas requiring high levels of security would have to be alerted of the presence of this technology and employ alternative methods of surveillance and anomaly detection that do not rely on digital cameras.

7 Conclusions

In this chapter, we presented a proof of concept implementation of a system for creating capture-resistant environments which prevents the recording of still images and videos of regions within that physical space, called BlindSpot. The system actively seeks CCD and CMOS cameras in the environment and emits a strong localized light beam at each device to neutralize it from capturing. Although the directed light interferes with the camera's operation, it minimally impacts a human's vision in the environment. This approach also requires no cooperation on the part of the camera nor its owner. In addition, we discussed how this work can be extended to permit certain cameras to take pictures in the environment while preventing others. Although the proof of concept implementation effectively blocks cameras within its 45° field of view up to 5–10 meters away, we can easily add additional detector and neutralizer units to prevent capture within a larger sweep. This implementation provided a platform for investigation of the challenges inherent to producing a capture resistant environment. We explained how our approach resolves many of these challenges and described potential extensions to this work to address others.

This work presents an implementation that can be optimized in the future to detect and to neutralize camera recording for a wider variety of situations including large environments and mobile entities, such as a person. Finally, we discussed various applications of BlindSpot, such as protecting intellectual property in industry labs, curbing piracy in movie theatres, and preventing the recording of high-profile individuals. As we discussed, although this technology has interesting applications potential, there are an equal number of concerns with such a powerful technology.

References

1. Art. 29 Data Protection Working Party. (2004) Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance. Document 11750/02/EN WP89, European Commission, http://europa.eu.int/comm
2. Brassil J. (2005) Using Mobile Communications to Assert Privacy from Video Surveillance. Presented at the 1st International Workshop on Security in Systems and Networks 2005.
3. Chung J. (2004) Threat of Subway Photo Ban Riseth Again. Gothamist, November 30, 2004.
4. Eagle Eye. (1997) Bulletin of the Connecticut Academy of Science and Engineering. Vol. 12, No. 2.
5. Halderman J.A, Waters B. and Felten E.W. (2004) Privacy Management for Portable Recording Devices. In the Proceedings of WPES 2004: 16–24.
6. Haro, A., Flickner, M., Essa, I.A. (2000) Detecting and Tracking Eyes by Using Their Physiological Properties, Dynamics, and Appearance. In the proceedings of CVPR 2000: 1163–1168.
7. Iceberg's Safe Haven. http://www.iceberg-ip.com/index.htm
8. Pilu, M. (2007). Detector for Use with Data Encoding Pattern. United States Patent Application. 20070085842, April 19, 2007.
9. Video Voyeurism Prevention Act of 2004. (2004) 18 USC 1801.
10. Wagstaff J. (2004) Using Bluetooth to Disable Camera Phones, http://loosewire.typepad.com/blog/2004/09/using_bluetooth.html