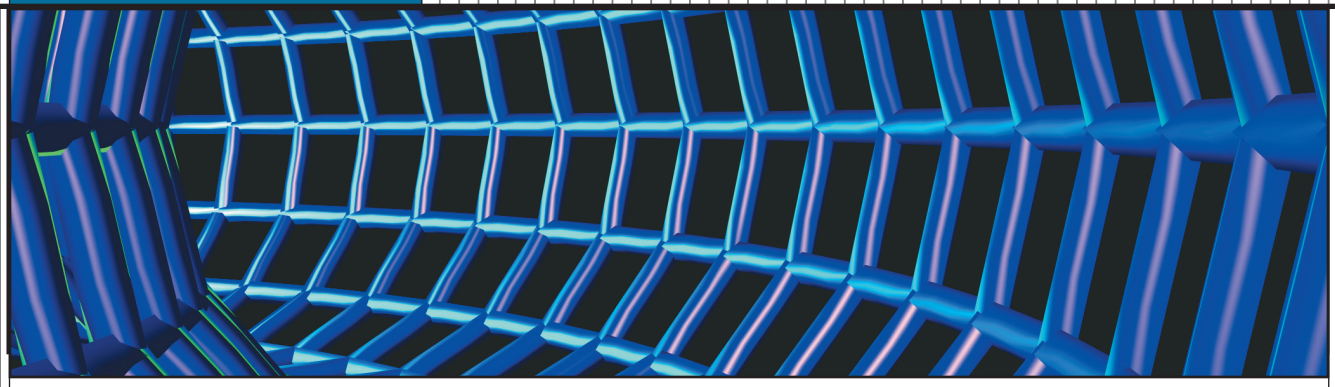


Dynamic Privacy in Public Surveillance

Simon Moncrieff, Svetha Venkatesh, and Geoff A.W. West
Curtin University of Technology, Australia

In implementing privacy protection in surveillance systems, designers must maximize privacy while retaining the system's purpose. One way to achieve this is to combine data-hiding techniques with context-aware policies governing access to securely collected and stored data.

In recent years there has been much discussion among researchers about privacy and its impact on ubiquitous computing.[1-6] While all agree that privacy is necessary in ubicomp systems, the field is still in its infancy. Several proposed systems implement privacy protection in ubicomp environments[2,3,7] but relatively few address privacy in what is possibly the first deployed ubicomp application: public surveillance. The most prominent is the Privacy Protected Video Surveillance (Privacy Cam) system designed by Andrew Senior and colleagues.[2]

However, this will soon change. Recent advances in surveillance technology, such as digital networked cameras and permanent storage solutions, are extending the scope of surveillance environments, transforming captured footage into indexed and searchable data. This will increase intrusion into privacy, which in turn will motivate the need to implement privacy measures to control access to surveillance data.

To be effective, such measures should be integrated into surveillance system design. Moreover, privacy policies applied to surveillance data should be altered dynamically in response to contextual factors to maximize privacy while fulfilling the system's purpose.

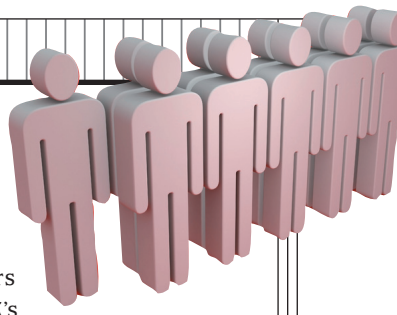
CONTROLLING INFORMATION FLOW

Several ubicomp researchers[4-6] have echoed the assertion of legal scholar Alan R. Westin that "no definition of privacy is possible," as privacy is highly subjective and dependent on goals or aims that are at times in conflict. For example, Jason Hong and James Landay[6] argue that "rather than being a single monolithic concept, privacy is a fluid and malleable notion with a range of trust levels and needs." This elusiveness has led to several theories about the nature of privacy.

Social psychologist Irwin Altman's privacy regulation theory[5] views privacy as a dynamic boundary regulation process in which individuals use various tools, including verbal and nonverbal communication, to control interactions with others to obtain their desired, thus optimal, level of privacy. This varies from person to person and changes according to the environment and circumstances. Boundary control fails if privacy is too great, resulting in social isolation, or too low, resulting in *crowding*—receiving more input than desired.

Controlling information flow is at the heart of Altman's theory, which can be applied to ubicomp by extending the tools used to control communication to include computational devices, such as sensors, within the environment.[5]

 Published by the IEEE Computer Society 0018-9162/09/$26.00 © 2009 IEEE



It likewise underlies Westin's definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[4]

Ubicomp researchers have come to the same realization.[3,6,8,9] For example, Victoria Bellotti and Abigail Sellen[3] identified the importance of control and feedback in implementing privacy protection in ubicomp environments—that is, users within the environment should be given control over the data captured within the environment as well as feedback on the processing, sharing, and use of this information. In a similar vein, Scott Lederer, Anind Dey, and Jennifer Mankoff[8] defined *everyday privacy* as "individual end users' ongoing exposure to and influence over the collection of their personal information in ubicomp environments."

Occupants of ubicomp environments do not control all the information communicated about them. While Altman's theory describes the negative impact of too much information input on privacy, it does not consider excessive information output. To address this, Jaakko Lehikoinen, Juha Lehikoinen, and Pertti Huuskonen[5] introduced the concept of *leaking*, the disclosure of data due to the unintentional or uncontrolled flow of information.

Leaking is especially problematic in surveillance environments, which can capture, store, and process a wide range of searchable data beyond occupants' control. Advances in surveillance technology are compounding the problem, resulting in increasingly intrusive applications. For example, cameras in LCD screen billboards can determine properties of people looking at the billboard such as age and gender, and surveillance systems in shopping malls can track customers' whereabouts through their mobile phones.

PRIVACY REQUIREMENTS

Privacy is highly subjective, varying across cultures and individuals. However, technology will be a unifying factor due to the loss of privacy that will result from surveillance.

Advocates of surveillance argue that people in a public space have no right to privacy due to the presence of others—that is, what someone does in public cannot be expected to remain private.

Nevertheless, there is a growing consensus that surveillance systems pose a danger to privacy that should be debated and, ultimately, mitigated by legislative action.[10] For example, in the United Kingdom a recent report by the Royal Academy of Engineering (RAE)[11] recognized the impact of evolving technologies on such systems and called for research to develop ways of monitoring public spaces that minimize the impact on privacy. Significantly, the report was authored by both RAE engineers and social scientists from the UK's Academy of Social Sciences.

Just as technology can positively or negatively impact society, so too does society influence technology. Researchers should develop privacy protection methods in conjunction with advances in surveillance technology to minimize the costs imposed by new legislative and regulatory requirements on the technology once it has been deployed. In addition, such methods should aim to maximize privacy while retaining the surveillance system's purpose. Such an approach requires a dynamic method for applying privacy measures, as a single measure would either restrict the purpose or fail to minimize privacy. To maximize privacy, the system must minimize the outward flow of information about occupants from the environment.

There is a growing consensus that surveillance systems pose a danger to privacy that should be debated and, ultimately, mitigated by legislative action.

To explore these requirements, we first examine the limitations associated with closed-circuit television (CCTV) systems, and contrast these with advances resulting from the move toward networked camera systems. We then consider why privacy should be integrated into surveillance systems as they are developed, and subsequently propose a design approach for maximizing privacy in surveillance systems.

CCTV: LIMITATIONS AND CONCERNS

Nowhere is the use of CCTV systems more established than in the UK. As of 2004, the country had some 4.3 million CCTV cameras like the one shown in Figure 1, approximately 15 percent of the total number of such cameras deployed worldwide.[2]

Traditional CCTV systems in the UK use analog cameras, which limit the amount of video data that can be stored and retrieved. In addition, the relatively poor quality of images, especially those captured by older cameras, can inhibit the data's usefulness—for example, as evidence against criminal suspects in court. Further, CCTV cameras are connected to closed networks controlled by a multitude of public and private organizations. The lack of standardization combined with policy differences

Figure 1. Nowhere is the use of CCTV systems more established than in the UK. Source for left image: www.flickr.com/photos/stephenjohnson/2899060572/sizes/0. Source for image on right: http:commons.wikimedia.org/wiki/File:One_nation_under_OCTV_1.jpg.

regarding the use of such systems can also make data retrieval problematic.

These technological and practical limitations have minimized CCTV systems' impact on privacy in the UK, which is arguably one of the freest societies in the world and thus particularly sensitive to threats to civil liberties. While the British public has expressed concern about CCTV systems, only a small fraction—1 percent of the population—has changed its behavior to avoid areas under surveillance.[12]

Despite the public's apparent ambivalence, numerous civil liberties groups have called attention to the privacy dangers of CCTV systems. Some organizations publicize the location of cameras so that people can travel through an area under surveillance without being caught on camera.[1] A proposed method for geotagging CCTV cameras enables mobile users to share the location and nature of surveillance systems with others.[13] Such approaches reduce privacy intrusion by allowing people to control, to some extent, their information leak.

The use of microphones in CCTV systems, the potential oversaturation of camera coverage, and human monitoring of surveillance footage have also aroused privacy concerns. Although such concerns have not entered the mainstream consciousness and forced CCTV system operators to implement more than the most basic privacy measures, generally relating to data access, this will change as technology advances.

THE CHANGING NATURE OF SURVEILLANCE

With analog CCTV technology, the inability to easily store, replicate, and process video footage limits information leak. However, this is no longer the case with emerging networked, digital surveillance systems. As information leak increases, without allowing those observed to have control or feedback over the surveillance, the potential for privacy intrusion will grow.

Numerous advances in digitization and networking technology will not only overcome the limitations of CCTV systems but also extend the scope of surveillance and, in doing so, increase its impact on privacy. Examples of this technology include the following:

- *Digital cameras*: Advances in image sensor technology will increase image quality while decreasing camera size.
- *Permanent storage*: The use of digital cameras, coupled with the decreasing costs of storage, will lead to the permanent nondegrading storage of captured digital data.
- *Rapid data retrieval*: The use of digital video will make it easier to index and retrieve data.
- *Mobile cameras*: Digitization and networking technology will enable surveillance cameras to be placed on mobile platforms such as public transport vehicles and aerial drones.

- *IP cameras*: The use of Internet Protocol, particularly wireless, technology will enable the more efficient networking of surveillance cameras, which will in turn facilitate their deployment and access to footage.

To illustrate how evolving digitization and networking technology has improved surveillance effectiveness, consider the following statistics: In the UK, CCTV systems generally help to solve only about 3 percent of crimes, but this figure is between 15 and 20 percent where more advanced technology and methods are in place.[14] Decreasing camera prices, in conjunction with wireless technology, have increased both the proliferation and quality of surveillance systems, particularly in places where CCTV is less prevalent, such as the US.[15] Organizations will be able to cost-effectively deploy newer, better systems and extend or replace older technologies—for example, expensive, mechanical pan-tilt-zoom cameras, with cheap, static, digital cameras with overlapping fields of view. To boost safety, select public transport vehicles in London are being outfitted with exterior and interior surveillance cameras that provide real-time images to authorities.[16]

Technology advances have also enabled multisensor surveillance. Cameras with omnidirectional microphones, which are not restricted by viewpoint, can be a powerful surveillance tool. Alternatively, directional microphones can be used to target audio—for example, a conversation—at a distance of about 100 meters. However, uncertainties in matching what the system sees with what it hears have aroused strong resistance to camera microphones by privacy watchdogs, who quickly introduced measures to limit their use.[17]

Advances in image processing will make it easier to search and interpret visual data captured by surveillance cameras. Law-enforcement agencies have deployed vehicle number plate recognition systems since the 1980s, and various government organizations are prototyping face-recognition systems using limited datasets.[18] Such systems ultimately have the potential to record a person's complete movements in time and space.

In concert, these evolving technologies move surveillance beyond the concept of a static, isolated camera "watching" a public space to an all-seeing eye that can convert an individual's everyday movements and habits into permanently stored, indexed, searchable data that can be processed in many different ways. The argument by surveillance advocates that people in a public space should have no expectation of privacy from a camera, which is merely another occupant in that space, no longer holds. The camera is not just another anonymous face in the crowd, but an entity following you around all the time.

INTEGRATING PRIVACY INTO SURVEILLANCE

As surveillance becomes increasingly intrusive, public opposition to these technologies will grow. Lawmakers will be pressured to force organizations that develop and deploy surveillance systems to incorporate additional privacy protections. However, because legislation tends to lag behind technology, such measures will inevitably inhibit preexisting systems' functionality. Designing surveillance systems with privacy in mind, rather than as an afterthought, will accelerate the adoption of privacy policies in surveillance and reduce the impact of enforced privacy measures.[6]

A surveillance system should deliver the maximum amount of data the observers require to achieve their purpose while minimizing intrusion on the observed.

For example, Google did not foresee privacy issues with Street View and thus did not incorporate privacy protections into the initial release of this feature in 2007. In response to public outcry, the company instituted several measures including the blurring of facial images and vehicle number plates and reducing image resolution to limit discernible information about pedestrians and vehicles. However, there is still considerable debate as to whether these measures go far enough; other identifying data such as location, clothes, and stature/gait are evident in Street View and may violate local privacy laws.

Privacy as an optimization problem

We view privacy as an optimization problem with respect to information flow. Assuming that people generally wish to reveal as little about themselves as possible, a surveillance system should deliver the maximum amount of data the observers require to achieve their purpose while minimizing intrusion on the observed. For example, providing those within a monitored environment with the highest degree of privacy would entail removing images of people from the video altogether, which would render the footage useless. Conversely, requiring everyone entering the space to submit to extreme identification methods, such as carrying a radio-frequency identification tag, would be socially unacceptable.

Applying this approach to Street View, we first consider the tool's purpose: to provide views of streets and buildings as an aid to navigation and exploration—not to observe pedestrians occupying the streets. Thus, to maximize privacy, ideally all pedestrian data should be filtered to remove identifying information. At the same time, to maximize its effectiveness, the system should have the highest image resolution possible.

Figure 2. In response to public outcry over the intrusiveness of its Street View feature, Google instituted several privacy-protecting measures, including the blurring of facial images and vehicle number plates and reducing image resolution to limit discernible information about pedestrians and vehicles.

Data hiding

The way most surveillance systems trade off data and privacy requirements is to first determine an appropriate privacy policy and then apply this to the data using a data hiding or abstraction technique.

Data hiding is achieved in video streams by detecting a region of interest that corresponds to privacy-sensitive information and removing or obscuring it. Faces, people, and license plates are common ROIs. Examples of this approach include removing images of people (and binary images representing their silhouettes)[7] or scrambling such images at different resolution levels.[19] As Figure 2 shows, the approach adopted by Google's Street View is to detect and blur vehicle number plates and faces within images.

Surveillance systems typically apply a single privacy policy and hide data by default, enabling only authorized persons to access the raw data. For example, if data hiding is implemented using image scrambling based on encryption, authorization could be in the form of possession of a relevant decryption key.[19] A more comprehensive approach proposed by Senior and colleagues limits access to three types of data according to the user's authorization level.[2] Law-enforcement personnel could access the entire video, "privileged" users could access a rerendered video with certain privacy-sensitive information removed, and "ordinary" users could access statistics—for example, the number of people in the monitored environment.

Context-aware surveillance

A single privacy policy is too restrictive to effectively balance the conflicting goals of maximizing surveillance functionality and minimizing privacy intrusion. The resulting system tends to be either too intrusive or limited in scope. What is required is a dynamic data hiding approach that adjusts the privacy policy over time to meet the observers' requirements while providing the observed with an acceptable level of privacy.

The observer's privacy-related goals can be incorporated into the system by accounting not only for the observer's trust level—that is, via authorization—but also the context in which the observer uses the system. For example, if the observer's job is to monitor crowd flow through an underground subway station to relieve congestion when it occurs, the observer does not need to access raw video footage. Rather, obscuring the foreground of the image frame with a single solid color would give sufficient details regarding the number of people present. The foreground indicates movement within the image, which in turn indicates people's motion through the scene. Such a technique could also be combined with motion analysis to provide more information regarding movement through the frame.

The system should also consider what is happening in the monitored space. By linking privacy measures to environmental context, such measures can be adjusted to changes or events. For example, in normal circumstances the system would provide a high level of privacy protection—say, by replacing people in the image with blobs or bounding boxes—but if an alarm activates, the system could reduce privacy protection to enable an observer to verify that the event was correctly detected and to take the appropriate action.

The concept of context-aware surveillance can be extended to include general indicators of environmental context. For example, because people often feel safer in crowds, the system could increase privacy protection as crowd size increases, as there is less need to monitor the crowd to ensure individual safety.

Contextual factors can thus be combined with data-hiding techniques to implement dynamic privacy policies that account for the observed as well as the observers—and in turn those who control the surveillance—while minimizing information leak.

Data equity

The RAE report[11] recognized the importance of reciprocity to the public's trust of surveillance, as it introduced an element of feedback into surveillance applications. In recommendation R7, the report stated that "in the case of camera surveillance, there should be debate on and research into ways to allow the public some level of access to the images captured by surveillance cameras."

The report highlighted the Digital Bridge project, designed to provide Internet access to residents of Shoreditch, East London, using IPTV. Among the services offered to the community was access to IP surveillance cameras in the area, cycling at 30-second intervals. This feature proved to be popular, with a higher proportion of residents viewing the surveillance footage than certain popular TV programs, and resulted in an increased reporting of crime. Other UK councils have implemented similar IPTV schemes but removed the access to surveillance cameras due to privacy concerns.[20]

There is a growing amount of surveillance data, both captured and stored, and if the privacy-sensitive components were concealed or removed, a wealth of valuable information could be obtained, particularly from cameras. For example, filtered surveillance data could be used to inform commuters about crowd density at train and subway stations. Municipal councils could monitor the usage of local public places and paths. Merchants could determine the amount of pedestrian traffic near their shops. Security, law enforcement, and emergency services personnel could dynamically bypass routes that go through crowded areas and thus respond to an event more quickly.

Researchers could also benefit from access to desensitized surveillance data. For example, by removing people from the video and analyzing the motion vectors through a scene, they could conduct pattern analysis of crowds over long periods.

The *Oxford English Dictionary* defines privacy as "a state in which one is not observed or disturbed by others." However, this definition is rather unhelpful when it comes to designing privacy measures for ubiquitous computing applications, as one of the main purposes of such applications is to observe.

The best way to think about privacy in this context is in terms of controlling information flow. In the case of ubicomp systems, information flows between people as they interact. In addition, people interact indirectly with their environment when they are monitored by sensors such as video cameras and microphones. It is information leak that results in the loss of privacy associated with ubicomp systems. Preventing the loss of privacy requires measures that stop or control information leak. This is especially true for surveillance systems, which by nature are intrusive and, with continuing advances in technology, are capable of capturing and storing increasing amounts of data.

When implementing privacy protection in surveillance environments, designers must minimize information leak while retaining the system's purpose. One way to achieve this balance is to combine various data-hiding techniques with context-aware rules governing access to securely collected and stored data. Adjusting the privacy policy according to the objective of the surveillance and the situation within the environment makes it possible to dynamically satisfy the needs of both the observers and those being observed.

While privacy is a social issue, the underlying cause of the loss of privacy due to surveillance is technological. Consequently, protecting privacy in monitored environments requires a sociotechnical approach. Reciprocity, or feedback, is one such approach that will increase trust in effective surveillance systems. C

References

1. A. Cavallaro, "Privacy in Video Surveillance," *IEEE Signal Processing Magazine*, Mar. 2007, pp. 168-169.
2. A. Senior et al., "Enabling Video Privacy through Computer Vision," *IEEE Security and Privacy*, May-June 2005, pp. 50-57.
3. V. Bellotti and A. Sellen, "Design for Privacy in Ubiquitous Computing Environments," *Proc. 3rd European Conf. Computer-Supported Cooperative Work* (ECSCW 93), Kluwer Academic Publishers, 1993, pp. 77-92.
4. S. Lederer et al., "Personal Privacy through Understanding and Action: Five Pitfalls for Designers," *Personal Ubiquitous Computing*, Nov. 2004, pp. 440-454.
5. J.T. Lehikoinen, J. Lehikoinen, and P. Huuskonen, "Understanding Privacy Regulation in Ubicomp Interactions," *Personal and Ubiquitous Computing*, Nov. 2008, pp. 543-553.
6. J.I. Hong and J.A. Landay, "An Architecture for Privacy-Sensitive Ubiquitous Computing," *Proc. 2nd Int'l Conf. Mobile Systems, Applications, and Services* (MobiSys 04), ACM Press, 2004, pp. 177-189.
7. J. Wickramasuriya et al., "Privacy-Protecting Data Collection in Media Spaces," *Proc. 12th Ann. ACM Int'l Conf. Multimedia* (Multimedia 04), ACM Press, 2004, pp. 48-55.
8. S. Lederer, A.K. Dey, and J. Mankoff, *A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous*

Computing Environments, tech. report UCB/CSD-2-1188, Computer Science Division (EECS), University of California, Berkeley, 2002.
9. X. Jiang, J.I. Hong, and J.A. Landay, "Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing," *Proc. 4th Int'l Conf. Ubiquitous Computing* (UbiComp 02), LNCS 2498, Springer-Verlag, 2002, pp. 176-193.
10. R. Lucky, "Zero Privacy," *IEEE Spectrum*, July 2008; http://staging.spectrum.ieee.org/telecom/internet/zero-privacy.
11. Royal Academy of Eng., *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, tech. report, Mar. 2007, RAE; www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf.
12. M. Gill and A. Spriggs, *Assessing the Impact of CCTV, Home Office Research Study 292*, Home Office Research, Development and Statistics Directorate, 2005; www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf.
13. J. Kiemer et al., "Spybuster—A Community-Based Privacy Tagging Platform," *Proc. 10th Int'l Conf. Human Computer Interaction with Mobile Devices and Services* (MobileHCI 08) ACM Press, 2008, pp. 491-492.
14. O. Bowcott, "CCTV Boom Has Failed to Slash Crime, Say Police," *The Guardian*, 6 May 2008; www.guardian.co.uk/uk/2008/may/06/ukcrime1.
15. A. Cameron et al., *Measuring the Effects of Video Surveillance on Crime in Los Angeles*, tech. report CRB-08-007, 5 May 2008, School of Policy, Planning, and Development, Univ. of Southern California; www.library.ca.gov/crb/08/08-007.pdf.
16. *Transport for London*, "Live CCTV Boost to Bus Safety," 22 Oct. 2008, Mayor of London; www.tfl.gov.uk/corporate/media/newscentre/10118.aspx.
17. P. Hennessy, "CCTV Camera Microphones to Be Axed," *The Sunday Telegraph*, 27 Jan. 2008; www.telegraph.co.uk/news/uknews/1576686/CCTV-camera-microphones-to-be-axed.html.
18. "Video Surveillance," 18 Dec. 2007, *Privacy International*; www.privacyinternational.org/article.shtml?cmd[347]=x-347-559088&als[theme]=Video%20Surveillance.
19. F. Dufaux and T. Ebrahimi, "Scrambling for Video Surveillance with Privacy," *Proc. 2006 Conf. Computer Vision and Pattern Recognition Workshop* (CVPRW 06), IEEE CS Press, 2006, pp. 160-166.
20. M. Ballard, "Living Room CCTV Feed Encourages 'Inappropriate Watching,'" *The Inquirer*, 30 Jan. 2008; www.theinquirer.net/inquirer/news/1035361/shoreditch-cctv-encourages.

Simon Moncrieff *is a research fellow in the Department of Computing at Curtin University of Technology, Perth, Western Australia. His research interests include computer vision, anomaly detection, and dynamic privacy covering smart homes and surveillance. Moncrieff received a PhD in computer science from Curtin University of Technology. He is a member of the IEEE. Contact him at s.moncrieff@curtin.edu.au.*

Svetha Venkatesh *is a professor in the Department of Computing at Curtin University of Technology, where she also directs the Institute of Multi-Sensor Processing and Content Analysis and codirects the Centre of Excellence in Intelligent Operations Management. Her research interests include large-scale pattern recognition, image understanding, and applications of computer vision to image and video indexing and retrieval. Venkatesh received a PhD in computer science from the University of Western Australia. She is a member of the IEEE. Contact her at s.venkatesh@curtin.edu.au.*

Geoff A.W. West *is a professor in the Department of Spatial Sciences at Curtin University of Technology and at the Cooperative Research Centre for Spatial Information. His research focuses on the processing and interpretation of spatial information, visualization, and privacy. West received a PhD in systems engineering from City University London. He is a senior member of the IEEE, a member of the Institution of Engineering and Technology, a fellow of Engineers Australia, and a member of the Australian Computer Society. Contact him at g.west@curtin.edu.au.*