The beneficial use of surveillance and computer vision to achieve safer and more secure urban environments justifies the privacy risks. Discuss.

Ramya Hebbalaguppe
School of Electronic Engineering
Email: ramya.hebbalaguppe2@mail.dcu.ie
Dublin City Univeristy, Ireland

15 June 2012

Surveillance is the principle of observing public or private places and then using such information to either provide additional safety and using the captured information to facilitate or enhance user experience. Depending on the users perspective the outcomes of surveillance may be positive or negative. As the following examples demonstrate, proper uses of surveillance bring many benefits to society and these outweigh the negative impact on privacy. Applications of video surveillance span several broad areas, both in indoor and outdoor environments. Some indoor applications could be at diplomatic missions, airports, hotel lobbies, school corridors, prisons for analysis of anti-social behaviour, and at departmental stores to prevent actions such as staff theft commonly termed as sweethearting. Some outdoor applications include environmental monitoring such as forest fire detection and tracking wild animals. Visual surveillance is also used where manual surveillance would be impossible such as in nuclear plants and military zones to counteract terrorism and crime. Urban surveillance, like vehicle license plate recognition, monitoring parking, speed control, people tracking and object recognition, improve efficiency and reduce costs.

While there is a broad spectrum of benefits listed above, with the proliferation of video surveillance systems across cities, many groups have raised privacy concerns on the use of such technology. In order to address these concerns, we need to study the factors that affect an individual or groups privacy. Privacy is an individual or group's fundamental right to disclose, withdraw or not provide any information about themselves. The degree and importance of the privacy depends largely on, among many factors, ones personality, country, age, and culture. Free availability of information often conflicts with a persons desired level of privacy. This is not only true for celebrities seeking a respite from paparazzi but is also true for many individuals as well. Some famous examples are the lawsuit filed by many countries against Google due to the Street View feature of Google Maps[1] and The Leveson enquiry[1] into unauthorised access to mobile phones. With every information and communication feature or technology update from social networking sites like YouTube, Facebook, geo-tagging on Flickr and Twitter, serious privacy issues have been identified.

For some applications where there is greater societal benefit, privacy may have to be compromised. Military applications or matters of national security typically may not always consider individuals privacy as the risks involved is far greater than a single persons privacy. Case in point, CCTV footage helped in capturing terrorists responsible for Mumbai attacks, November 2008 and Al-Qaeda leader responsible for 9/11 terrorist attacks in the US. Two unexploded bombs were found in luggage aboard two trains in Germany, August 2006. Terrorists were arrested as a result of video footage being recorded. Video surveillance has helped to reduce the number of security personnel or police officers who had to walk around the blocks in the city constantly. Advances in computer vision allow automatic analysis of scenes which can lead to recognition of people in a monitored area. The beneficial aspect of video surveillance is primarily safety and timely intervention and it reduces response time by law enforcement personnel or medical professionals in case of incidents or accidents.

We need to revisit our perception about privacy and redefine the levels and the laws governing our right to privacy. In other words, we will have to work amicably in balancing the privacy issues, and the functionality and features of surveillance[2]. In the following sections, some of the advances in video surveillance that threaten privacy are highlighted together with how emerging technologies like computer vision and cryptography can work hand-

[1] http://www.levesoninquiry.org.uk/

in-hand to protect privacy while reducing the security risks[3].

Privacy threats and potential abuses of surveillance: The diffusion of camera networks, tiny sensors, increased availability of storage capabilities and accessible has made it a lot easier to gather information about an individual thereby increasing the risk of misuse and abuse of surveillance data such as criminal misuse by law enforcement officers. The American Civil Liberties Union has outlined a number of concerns around video surveillance[4] like criminal abuse, institutional abuse, abuse for personal purposes discriminatory targeting, and voyeurism. These issues are further amplified with high definition cameras and face recognition software. For example, four council workers in Liverpool used CCTV pan-tilt-zoom cameras to spy a woman in the apartment. The other examples include police officers helping friends stalk women [5][6].

Some advances in video surveillance to protect privacy:

Fully automatic surveillance: Automated surveillance could be used to overcome misuse of video data used by unauthorised people albeit with higher false positives due to absence of intervention of human operators. Smart cameras can be used to embed privacy constraints in design of video surveillance systems, for example, they can be programmed to mask, identify and deidentify region of interest (ROI) and scramble information. The latter could be achieved both in the image/transform and bit stream domains. Pixelation is commonly used in television news and documentaries in order to obscure the faces of suspects, witnesses to preserve their identity; Alternatively, Gaussian blur is used to smooth out ROI. Scrambling is also a part of standards JPEG2000 and MPEG-4. Scrambling in H.264 is already available as a product[2], whose input is analog video but outputs a compressed H.264 using scrambler. Unscrambling can be allowed in higher authorities like advocates, police in criminal investigations. A real-time approach to preserve privacy while not compromising the ability to observe actions and obscuring individual identities is presented using respectful cameras in[7][8].

Privacy through obfuscation: MPEG-7 standard describes a scene in terms of semantic objects where we record needed information from the scene.

[2] For example, Emitall Surveillance, Switzerland

Privacy sensitive zones can be concealed for example, bank teller, casino tables, windows and doors - legal solutions are close to maturity and have been productised[3].

The critical need to provide privacy and security assurances for distributed multimedia sensor networking in applications including military surveillance and healthcare monitoring are discussed in[7]. An efficient framework to carry out privacy preserving surveillance which is not only computationally efficient, but also addresses legal issues is presented in [8].

User Controlled privacy: A system prototype for privacy enhancement in video surveilled areas by integrating computer vision and cryptographic techniques into networked building automation systems has been presented in [11]. People in a video stream control their visibility to allow either the real view or an obscured image to be seen. The parts of the video stream that show a person are protected by a cipher and can be sent over untrusted networks. Some services like “Friends can check me in Places” feature could be turned off or provided only as an opt-in feature on a smart phone to prevent abuse from applications.

There is a need for a more uniform international privacy policy especially in the dissemination of multimedia content that distinguishes between civil and military privacy issues. It is important to understand and set protocols for trustworthiness, accessibility of the data-gatherer and length the data is stored for. Several countries in the European Union have set up or are in the process of setting up directives and guidelines to regulate video[4]. There has already been research done to evaluate the performance analysis of privacy protection solutions. It is paramount to validate privacy protection solutions against user and system requirements using subjective and objective evaluations.

Conclusion: A quote by an American writer, Stan Lee, “With great power there must also come - - great responsibility!” relates well even to the beneficial use of surveillance. I firmly believe that surveillance offers advantages that overweigh the privacy risks when used responsibly. There is an increasing need for users to be aware of privacy implications of any surveillance technology so as to make informed decisions about being a part of it. Like-

[3] such as - Eptascape Inc, USA

[4] EU Directive 95/46/EC

wise, a surveillance authority has to be responsible and respect individuals privacy as is humanly possible, either by educating the need for it or providing privacy controls for users. An interdisciplinary research between signal processing researchers and social sciences is required to adapt the requirements from citizens demands to privacy. An acceptable compromise could be achieved with the responsible usage of surveillance technology. I believe that it is possible to have the best of the surveillance and privacy in systems in the near future.

References

[1] S. Bellah (2011), Google Street View: Invasion of Privacy or Pertinent Publication? The Conflict of the Right to Privacy With Freedom of Speech in the International Community.

[2] Dufaux, F. and Ebrahimi, T.(2006), Scrambling for Video Surveillance with Privacy. Computer Vision and Pattern Recognition Workshop, p. 160.

[3] A.Senior , S. Pankanti , A. Hampapur , L. Brown , Y. Tian , A. Ekin (2005), Blinkering Surveillance: Enabling Video Privacy Through Computer Vision. IEEE Security and Privacy.

[4] A. Cavallro (2007), Privacy in Video Surveillance.IEEE Signal processing Magazine. p. 168.

[5] Dufaux, F and Ebrahimi, T. (2008), Scrambling for Privacy Protection in Video Surveillance Systems. IEEE Transactions on Circuits and Systems for Video Technology, vol.18, no.8, pp.1168-1174.

[6] Kundur, D.; Luh, W.; Okorafor, U.N.; Zourntos, T. (2008) , Security and Privacy for Distributed Multimedia Sensor Networks. Proceedings of the IEEE , vol.96, no.1, pp.112-130.

[7] Schiff, J, Meingast, M., Mulligan, D.K., Sastry, S., Goldberg, K., Respectful cameras: detecting visual markers in real-time to address privacy concerns. Intelligent Robots and Systems, 2007. IROS 2007. IEEE/RSJ International Conference on , vol., no., pp.971-978.

[8] Upmanyu, M. Namboodiri, A.M. Srinathan, K. Jawahar, C.V. , Efficient privacy preserving video surveillance. Computer Vision, 2009 IEEE 12th International Conference on , vol., no., pp.1639-1646.

[9] Newton, E.M. Sweeney, L.Malin, B. , Preserving privacy by de-identifying face images. Knowledge and Data Engineering, IEEE Transactions on , vol.17, no.2, pp. 232- 243.

[10] J. Coutaz , F. Brard , E. Carraux , W. Astier , J. L. Crowley, CoMedi: Using Computer Vision to Support Awareness and Privacy in Mediaspaces. In Proceedings of ACM conference on Computer-Human Interaction (CHI), 1999

[11] S. Torsten, W.Christoph, H. Ludger, R. Daniel, V. Luc and S.Andreas, Privacy in video surveilled areas. Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services