The Social Impact of Computer Vision

Topic 1: Urban Landscapes

by

Vittal Premachandran
vittalp@pmail.ntu.edu.sg
School of Computer Engineering
Nanyang Technological University, Singapore

300,000 cameras were watching the visitors of the 2008 Beijing Olympics. There is an estimated one CCTV camera for every 14 people in the UK. An average Briton passes under 300 cameras a day. Such"staggering" statistics is bound to be a common feature in most of the developed cities of the world. These cameras capture your face, identify the emotion behind them, follow you as you walk along the streets, track your actions, and store them all in a database that can be accessed at any point of time in the future. Is such a level of surveillance a necessity, or is it just plain infringement of privacy?

Ever since the gruesome attacks on September 11, 2001, there has been a wide-ranging debate over the beneficial use of surveillance and the extent to which an individual has to forgo his/her personal privacy for the sake of national security. The threat of terrorism, and the magnitude of disaster caused by terrorist attacks on urban landscapes, has forced government institutions to rethink their security strategies and lean towards more sophisticated surveillance mechanisms. The nature of these attacks means that every urban community, and country at large, has to be ready for such attacks well in advance. Having disaster management strategies that come into effect after an attack has taken place is inadequate. The most obvious preemptive technique that one can think of is public surveillance, and it is hard for one to argue against its benefits.

Back in the days when terrorism was not that big a threat, there were other dangers that people wanted protection from. Villages, and towns, appointed guards to look out for stray wild animals and thieves. As industrial revolution helped towns

expand into cities, the effectiveness of localized guards started diminishing and hence there was a need for the establishment of a more coordinated city police. As cities expanded further, people started looking towards more technologically advanced, and automated, surveillance technologies that augmented the traditional police. Today, a CCTV camera is present almost everywhere. There are cameras in supermarkets, schools, lifts, banks, libraries, subways, highways, and, people are even installing CCTV cameras at their homes!

The origins of surveillance are well-founded and there is no doubting its effectiveness. Security cameras help stop crime, and that is a fact. The very presence of a security camera instills fear among the public and prevents them from committing crime. While a CCTV camera can catch a shoplifter red-handed, a speeding camera can identify over speeders. A recent example of the beneficial use of CCTV cameras is its current use in London. The hundreds of CCTV cameras installed in the city are helping the police arrest the people who sparked, and participated in, the Tottenham riots.

With the acknowledgement of the benefits of public surveillance, we are left to decide if its merits outweigh the demerits. The biggest hurdle in the path of surveillance technologies is that they are perceived to be invaders of personal privacy. We have debates that are designed to question whether the benefits of surveillance justify this apparent invasion. The very fact that we are trying to pitch in security versus privacy suggests an acceptance on our parts that one has to give way to the other. Rarely does anyone ask why this has to be so. As Bruce Schneier, a computer security specialist, argues in his article [1], "Security and privacy are not two sides of an equation", and they never should be! Why should the enhancement of public security account to us forgoing our personal privacy? The debates should not be about whether or not surveillance justifies privacy risks, but should be about how to make automatic surveillance fall within the constitutional realms of a country.

Benjamin Franklin cautioned more than two centuries ago saying, "they that can give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety." While the quote might look extreme in current context, the spirit of the comment is what matters. Personal privacy is one's fundamental right, and any amount of surveillance should not deprive us off it. Technology has a lot of good to offer, if used in a proper way. The unfortunate fact about technology is

that it is very easy for someone to misuse it. Hence, we need strong governmental regulations, which regulate the use of public data. We need to identify a method of providing security and respecting one's privacy. This can be done by rewriting our laws and redesigning our systems.

Laws that we have today were crafted decades ago, when the dynamics of the world was vastly different from what it is today. Laws are not keeping pace with the rate at which technology is growing. Moreover, many current day systems are designed with hardly any thought given towards security and the protection of the users' rights. When they are later found to be lacking in security, the holes are "patched". When security is tacked on an already designed and functioning system, the method of achieving it is usually invasive from a privacy perspective. Invasive patches are thought of as the only solution to make the systems more secure, and that is the reason why we have people believing that they have to abandon their privacy for vague promises of security. What we are not being told is that we can have both. If security and privacy are incorporated into the architecture from the beginning, it can lead to a mutually reinforcing system from the perspective of operations, security, and privacy [2].

Not only should there be a rethinking of the system, but the authorities who handle our data should also take steps to exude a sense of trust among the public. People are currently wary of the government and third party institutions snooping into their personal data, and suspect them of misusing their power. Sadly, not many steps are being taken to reduce this trust deficit. There is already a lot of information being collected, and stored, without one's knowledge. The EZ cards installed in your cars tell the system where you are traveling, the mobile phone that you carry allows telephone companies to triangulate you, the credit/debit card payments that you make allow the card-issuing companies to look into the commodities that you buy, your work computer can keep track of your browsing history, and now, CCTV cameras follow you as you walk down the road.

Is it actually necessary for someone to collect so much personal data? Collecting tons of data, using the above means, usually serves no purpose. Focused data collection should be the norm and not broad surveillance of everyone. A lack of focused data collection boils down to a lack of planning during the system's architecture design. Privacy is something that does not naturally occur in most systems; they must be deliberately architected. System designers should be made

aware of the importance of protecting an individual's privacy. Systems should be developed such that they analyze the data and keep only the most relevant part of it. In addition, once the data has served its purpose, it should be deleted and not stored in databases, indefinitely.

Most digital data that is generated is hard to wipe out. More and more of our online communications are becoming less ephemeral. Google, for instance, stores all your emails, chats, and, browsing and search history. We do not want this to be happening during video surveillance. People feel violated if their personal information is taken without their permission. Misuse of data has become easy, as normal constitutional protections do not apply to a lot of the digital world. While a police might need a court-issued warrant to search someone's home, or tap into someone's phone conversation, they can easily issue a subpoena to a third-party company, asking for data that they have stored about us. Hence, we need to build in mechanisms that would help us identify who is looking at the data and assure the public that their data is not being misused. We need to ensure that the world does not become a large security area, where the slightest joke, made years ago, lands us in a soup.

If history is anything to by, it is highly unlikely that the advancements in technology, and thus its use in public life, is going to wane down because of privacy issues. Therefore, we as researchers have a huge responsibility to ensure that the government, or any other third party, does not misuse our innovations and products. As computer vision researchers, we have a special responsibility towards the public, and our children, to build surveillance systems that future generations will be proud of. I feel that there is a necessity to do research keeping in mind societal values, expecting misuse of data, and ensuring that we do everything in our capacity to protect the user's basic human rights. All of this might look like a challenging task. However, we researchers do love a challenge, do we not?

References

[1] Schneier, B. (2001). Protecting privacy and liberty. In *Nature*, Nature Publishing Group.

[2] Clark, J.G., Beebe, N.L., Williams, K. and Shepherd, L. (2009) Security and Privacy Governance: Criteria for systems design. In *Journal of Information Privacy and Security.*