Brady Prize Essay Submission

David A. Mély
Brown University
david_mely@brown.edu

Topic 1: **Urban Landscapes**
The beneficial use of surveillance and computer vision to achieve safer and more secure urban environments justifies the privacy risks. Discuss.

Terminator rising

New technologies in computer vision—e.g., object identification as well as biological motion detection—are the building blocks to (not-so-) futuristic security systems and other devices involved in our well-being. We can now clearly envision a society where it is technically possible to precisely identify individuals in public space, what they are doing, when and where. Computer vision enhances the experience of human-machine interaction, but also challenges us to redefine privacy in societies where such devices become ubiquitous. Distinct point of views should be pondered: the more traditional view that privacy be a bulwark of individual freedom erected in reaction to ever-encroaching governments; thus thwarting the latter would safeguard the former. The reverse opinion could be qualified as "ecological": privacy is part of a social climate from which governments of more or less authoritarian nature stem. Then computer vision, rather than a mere tool at the disposal of varied institutions, could bring about important societal upheavals. It is our responsibility as scholars of this discipline to have an honest reflection on the long-lasting changes that it could effect.

Is privacy jeopardized when nobody is watching?

A common opinion on what the progress of surveillance systems entails is an undesirable loss of privacy. However, it also brings a blessing in disguise: as computer vision programs get more autonomous, being able, for example, to extract semantic sense out of recorded scenes, they reduce the need for human involvement and viewing of the records. Indeed, a justification today for the police authorities to have extended access to records would be to be able to garner data about some crime, because the human mind is yet unmatched in this task. Ideally, an advanced enough machine vision device would be able to reliably provide potential crime scenes or results of semantic searches—e.g., "look for: man in green sweater with a handbag from last Monday until today"—while restricting access to all the other parts of the record. Thus, progress in computer vision could usher in an era of greater accountability when handling such sensitive data.

Moreover, another common claim raised to attenuate the negative impact of advanced surveillance systems is that any person in public space has a low expectation about their own privacy, regardless of the

presence of CCTV cameras. Hence, trading off what remains of their privacy for the benefit of public security would be perceived as sound, especially in large public spaces where personal privacy is very low and anonymity—e.g., of potential terrorists—is very high.

Should it still be a concern?

However, the loss of privacy brought about should still raise stringent concerns for reasons specific to computer vision, and not just out of considerations of effectiveness (CCTV cameras have been claimed to displace crime to non-covered areas rather than reduce it). A technical safeguard against the effective misuse of the records that exist, and a reason why much more of these are not created yet, can be summarized as the problem of "big data". It is tremendously difficult to find a way through the welter of all visual data; most often, human intervention is still needed to interpret interesting contents, if only to find them among all the records that exist for a given surveillance device. The advent of machine vision that could autonomously interpret contents from records and could semantically organize them for presentation to a human decider would remove this restriction. Hence, computer vision poses serious ethical problems when it transforms raw data into a semantic data, i.e., a file possibly involving personal identities.

Furthermore, the end of the aforementioned "anonymity-by-big-data" could have pernicious social psychological effects. Indeed, privacy is known to play a critical role in stabilizing society (see Schwartz, 1968), by allowing deviations from normative behavior to remain private and not "contaminate" public space. The gap that separates terabytes of videos of individuals passing through an anonymous crowd and a computer vision system capable to annotate or make sense of such "big data" is also the gap that separates a raw video record from a file[1], even computer-generated. Public knowledge of the latter's existence, even though it would not affect private space at first, could lead to increasing tension towards uniformity of behavior. Authoritarian regimes know very well how a global sense of privacy deprivation can be wielded to achieve the regime's domination on society, be it in the manner of Orwell's "1984" or Huxley's "Brave New World"—both of which are characterized by drastic loss of privacy, though very differently: generalized surveillance as for the former, and an enforced hedonistic society where all form of art[2] is banned for the latter. The outcome, however, remains the same.

[1] In 1967, the Supreme Court of the United States of America ruled in "Katz v. the United States" [389 U.S. 347], nonphysical or "electronic" intrusion, such as wiretapping, was to be considered as a search, hence as an violation of personal privacy regulated by the Fourth Amendment of the constitution of the United States of America. There is no doubt that "intelligent" records, i.e., records that have been reorganized by a computer vision system capable of object and action identification, could be subject to very similar legal conflicts.

[2] It can be argued that art sometimes expresses the unutterable and often presents diverging interpretations; in any case, power-hungry regimes of all sorts were not mistaken when they tried to rein in the idiosyncratic aspect of its experience and define some sort of "official" or "authorized" art (e.g., as in Nazi Germany or Stalin's Soviet Union).

Although Orwellian dystopias remain the main hobgoblin evoked by the unchecked technological progress of computer vision, the previously evoked menace of internalized privacy loss might be more adequately described by dystopias à la Huxley. This kind of privacy encroachment is not directly related to surveillance systems but depends as well on progress in computer vision, and is best embodied by interactive advertising and other similar entertainment systems. Interactive advertising uses the state of the art in computer vision, as surveillance systems do, to guess the watcher's identity and classify it—in the sense of machine learning—to present personalized content. The content's degree of customization depends of course on the precision of the sponsor's classification, which may in turn reflect all kind of stereotypes—i.e. those harbored by the designers of such systems. Such a fact shows that those considerations do not pertain to the realm of mere technical or engineering details but also constitute a societal issue as these are broadcast to a large audience.

A screen set up in public space equipped with a camera and computer vision software may embody this new generation of advertising. But it may also present itself in the form of a sensor connected to a television screen[3], which shows that even living rooms, traditionally private, are now within the reach of computer vision and of the paradigm shifts this technology may thus effect more drastically. Various thinkers had foreseen this problem, from Ray Bradbury's "parlor walls" (Fahrenheit 451), representing the forced standardization of society through ever-present entertainment, to Alexis de Tocqueville's grim prophecy that future despotic regimes may rule peoples by the soft power of entertainment, guiding them towards "petty pleasures". Computer vision would be a key technology to implement a truly interactive environment effecting the aforementioned changes[4].

"Resist the beginnings, and consider the end."

In conclusion, this stern warning might be relevant to computer vision, whose amelioration of surveillance systems may as well reduce privacy as make much too potent tools available to their abusive use by institutions. However, we have tried to argue that even in the absence of an actively malevolent government, further progress in computer vision may perennially change man's psychological and social environment for worse as the tool shapes its user's mind as much as the mind had shaped the tool. We do not advocate a 21st century brand of Luddism; however, the need to educate about these technologies and (re-) introduce intellectual distance between man and its ubiquitous virtual environment is urgent. In the end, shutting down one school might be far more dangerous than a thousand more CCTV cameras in our streets.

[3] Cf. Microsoft's interactive advertising platform NUads for its popular Kinect for XBOX360™ device.
[4] What Italian philosopher Raffaele Simone calls the "meek monster", alongside with other aspects of the misuse of modern technologies.

References

Bradbury, Ray. (1953). Fahrenheit 451.
Huxley, Aldous. (1931). Brave New World.
Orwell, George. (1949). Nineteen Eighty-Four.
Schwartz, Barry. (1968). The Social Psychology of Privacy. *American Journal of Sociology*, Vol. 73, No. 6 (May, 1968), pp. 741-752
Simone, Raffaele. (2008). The Meek Monster: why the West is not going left.
Tocqueville, Alexis (de). (1840). Democracy in America.