: Can decision support improve surveillance and increase privacy?

by Daniel J. Power

Editor, DSSResources.COM

Some people assume that computerized decision support can help law enforcement use surveillance to detect crime and aberrant behavior, but only by invading the privacy of individuals. Surveillance involves monitoring behavior, activities, or other changing things to manage, direct, or protect people. Monitoring for aberrant behavior is the greatest privacy concern. This phrase, "aberrant behavior", refers to any behavior that deviates from an unwritten norm or standard. Defining aberrant and detecting such behavior may invade personal or group privacy. This topic is timely because machine learning and other Artificial Intelligence (AI) and statistical models are using data from closed circuit television (CCTV) cameras and other "big data" sources to analyze what people do in real time.

Hagen et al. (2018) argue "Organizations and their actors are increasingly using video surveillance to monitor organizational members, employees, clients, and customers." Surveillance and privacy are both societal/national/local and organizational issues. The dynamics differ in each setting, but the ethical issues and the possibilities are very similar.

Decision support algorithms are creating a more powerful form of automated surveillance (Power, 2014; 2016). Identifying aberrant behavior is the most subjective and potentially the most intrusive type of search and surveillance. Identifying observable crimes using CCTV data is generally more objective and less of a threat to privacy.

For example, if a decision support algorithm identifies a person using data from a surveillance camera who is entering a bank after midnight, and the algorithm then concludes that a crime is in progress and alerts a police supervisor or even directly dispatches a patrol unit to the area to check for more information seems prudent and reasonable.

On the other hand, if a decision support algorithm identifies a person using data from a surveillance camera who is entering a public restroom after midnight, and the algorithm then concludes that the person is acting suspiciously and alerts a police supervisor or even directly dispatches a patrol unit to the area to check for more information those actions seem a bit paranoid and perhaps unreasonable and even an infringement on personal liberty and privacy.

Should people expect privacy and freedom from surveillance? If so, when? Does privacy imply that

in some situations a person is not observed or disturbed by other people, cameras or recording devices? Is privacy only limited to behaviors in one's own home? The Merriam-Webster Online Dictionary defines privacy as "freedom from unauthorized intrusion and the quality or state of being apart from company or observation." Privacy also refers to being left alone and to being able to keep certain acts and information especially personal matters to oneself and avoid public attention. According to the International Association of Privacy Professionals (IAPP), "information privacy is the right to have some control over how your personal information is collected and used". When does surveillance invade a person's privacy?

People can choose to "give up" their privacy to machine surveillance when they perceive a benefit. For example, Alexa devices from Amazon for security and home security monitoring can improve both safety and privacy. The obligation of vendors is to insure appropriate use and confidentiality of the passively collected data. The same is true for automated face-to-face shopping in an Amazon Go store where surveillance cameras and computers automate shoping from when you enter with your smart phone to when sensors know you have left the store and automatically charges you for the items you walk out with.

According SAS, "Machine learning is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention." Machine learning assisted surveillance can detect crimes, increase security, and automate tasks.

Technology is improving, cf. Power (2016). For example, Genetec (2017) has a product called Citigraf that "collects and manages information provided by integrated CAD (Computer Aided Dispatch) systems, CCTV footage, ALPR data, RMS (Record Management Systems) and more, to immediately identify and display the exact location of an event using icons on a map from a built-in geographical information system (GIS)." Automobile insurers are increasing tracking, monitoring and when appropriate rewarding driving behavior, cf. Demarest (2006).

Ethical and responsible use of Artificial Intelligence (AI) and surveillance can have beneficial uses. Organizations should conduct ethics training for their technologists and have ethics committees in place to review the use of AI, cf., Forbes Insights (2018). Rules and models for using surveillance data in real-time must be carefully crafted and validated and determined to be necessary and reasonable. Context matters in assessing the surveillance data so the place, time of day, and weather conditions where the data is originating among other factors must be considered in processing streaming data. Rule developers and machine "trainers" need to be careful to avoid incorporating spurious or stereotyped generalizations.

Knowledge-driven decision support and decision support algorithms can potentially improve the speed and accuracy of surveillance, but poorly designed systems can decrease privacy and infringe on individual rights. Privacy impact assessments (Clarke, 2009) should be included in the System Analysis and Design process, as well as periodically once implementation is completed.

References

Camacho-Collados, M. and F. Liberatore, "A Decision Support System for Predictive Police Patrolling," Decision Support Systems, May 2015 DOI: 10.1016/j.dss.2015.04.012.

Clarke, R., 2009, “Privacy impact assessment: Its origins and development”, Computer law & security review, 25(2): 123–135 https://doi.org/10.1016/j.clsr.2009.02.002 .

Demarest, M., "The dawn of the always-under-surveillance age," email to D. Power and others, Friday, October 6, 2006 (see below).

Forbes Insights, "Organizations are gearing up for more ethical and responsible use of Artificial Intelligence," SAS Press Release, Sept. 18, 2018 at URL http://dssresources.com/news/5035.php.

Genetec Press Release, "Genetec announces Citigraf: New Public Safety decision support system," Genetec, October 13, 2017 at URL http://dssresources.com/news/5034.php

Hagen, C. S., L. Bighash, A. B. Hollingshead, S. J. Shaikh, K. S. Alexander, "Why are you watching? Video surveillance in organizations," Corporate Communications: An International Journal, Vol. 23, Issue 2, 2018. pp.274-291, https://doi.org/10.1108/CCIJ-04-2017-0043

N.A., "Privacy," Merriam-Webster Online Dictionary access 7/26/2018 at URL https://www.merriam-webster.com/dictionary/privacy

N.A., "What does privacy mean?" International Association of Privacy Professionals (IAPP) last accessed 7/26/2018 at URL https://iapp.org/about/what-is-privacy/

Power, D. J., ""Big Brother" can watch us," Journal of Decision Systems, Volume 25, 2016 - Issue sup1, pages 578-588 https://doi.org/10.1080/12460125.2016.1187420

Power, D. J., "Using 'Big Data' for analytics and decision support," Journal of Decision Systems, Volume 23, 2014, pages 222-228 https://doi.org/10.1080/12460125.2014.888848

SAS Analytics Insights, "Machine Learning: What it is and why it matters," at URL https://www.sas.com

van den Hoven, J., M. Blaauw, W. Pieters, and M. Warnier, "Privacy and Information Technology", The Stanford Encyclopedia of Philosophy (Summer 2018 Edition), Edward N. Zalta (ed.), URL = .

Marc Demarest email, subject: The dawn of the always-under-surveillance age, date: Fri, Oct 6, 2006 at 9:25 PM:
<br

This is NOT a spoof. I think I even know the guy who sold them on the idea...You were there when the first blood-red rays of the surveillance sun shot over the horizon, blinding you....

"Using driving data from the pilot, the United Kingdom's largest insurer has developed "Pay As You Drive" insurance, the first policy to help motorists control the cost of their insurance by making informed choices about when, where and how often they use their car. Pricing for "Pay As You Drive" insurance begins from as little as a penny per mile.

In-car GPS devices allow Norwich Union to build the insurance policy around each individual motorist. Customers will receive monthly bills based on car usage, including time of day, type of road, and mileage - another first in motor insurance. Bills will look similar to mobile phone bills, with the premiums for each trip calculated and totalled. This transparent approach to auto insurance will help customers control their insurance costs in a way

that's not been possible before now. "

I am sure somewhere in their marketing collateral there is the identifying phrase of the cryptofascist:

"If you don't have anything to hide, you have nothing to fear from this program."

Please cite as:.

Power, D., "Can decision support improve surveillance and increase privacy?" Decision Support News, Vol. 19, No. 19, September 16, 2018 at URL http://dssresources.com/newsletters/480.php.

Author: Daniel Power
Last update: 2018-09-22 04:22