International Working Group
on Data Protection
in Telecommunications

675.51.11

Working Paper on Intelligent Video Analytics

58th Meeting, 13-14 October 2015, Berlin (Germany)

Scope

Increasingly, intelligent video analytics[1] technologies are being used to detect and track individuals in order to deliver customized advertising, enhanced security, and customer management solutions. They do this by providing detailed audience measurement information and offering new channels and media to communicate with individuals. For example, the digital signage market is expected to be worth $23.76 Billion in 2020, growing rapidly at a compound annual growth rate of 8.18% between 2015 and 2020[2].

This paper addresses the use of intelligent video analytics technologies by both private and public sector. The technologies that are the subject of this paper are used to detect and/or track individuals and objects, but not to identify them. This paper applies to upgrades to existing video surveillance systems, standalone “smart CCTV” or digital signage systems through the addition of intelligent video analytics capabilities, as well as new, purpose-built systems incorporating these technologies. This paper explores the privacy implications of these technologies and provides recommendations for transparent and privacy-friendly implementations.

Other technologies that aim to identify individuals by using video technology and computer vision, such as biometric face recognition or number plate recognition systems, are beyond the scope of this paper. They are dealt with only to the extent necessary to show the difference regarding their privacy implications as they are subject to special privacy considerations.

[1] Other terms include video analytics, video content analytics, anonymous video analytics, digital signage, digital audience measurement/audience targeting, Digital-Out-Of-Home (DOOH) advertising/networks.

[2] See: http://www.marketsandmarkets.com/PressReleases/digital-signage.asp. Digital-Out-Of-Home advertising, i.e. advertising that reaches the consumer while they are outside the home (in public places, in transit, in waiting rooms, and/or in specific commercial locations such as shopping malls) is consistently growing while newspaper, magazine and radio advertising are losing ground.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

It should be noted that significant privacy and data protection implications and effects on other human rights exist even if the aim of the technology is not to identify or single-out individuals whose image is captured by the cameras[3].

Background

While user tracking and personalized advertising on the Internet[4] are already common place, such data-backed approaches to audience measurement are not yet as well developed in out-of-home advertising and personalized "offline" display advertising (digital signage) to consumers in the real world. Billboards, even digital ones, are not used to provide basic socio-demographic and usage metrics common to other forms of online advertising such as information on who is watching the ad and for how long and to determine the success rate of a particular ad campaign. Furthermore, "ordinary" CCTV systems used for security purposes are not able to tell if there is a person in front of the camera, whether a protected object has been stolen or which are the most visited parts of a particular store or shopping mall. Intelligent video analytics technology is capable of providing this information. In the near future, we can expect billboards to know when and how long we are looking at them, to know our age and gender. Smart CCTV and digital signage systems are able to manage networks of sensors and displays and offer new options for audience measurement and interaction with consumers.

There is also an increasing interest in so-called interactive advertisements which will combine digital displays with motion detection systems to entice the individual to interact or play with the advertiser - a gamification of advertising.

Intelligent video analytics enables a range of organisations including retailers, museums, airports and advertisers to better ascertain the types of individuals they encounter, to better adapt their services to them and to communicate with them more effectively. By being able to detect and track faces and objects in front of a camera or a display and to estimate some of their information (such as age, gender, movement and attention span data, etc.), intelligent video analytics may be used for the following purposes:

MANAGEMENT

- visitor counters,
- detection and optimisation of frequent routes, heatmaps for shop-floor and shelf optimisation,
- audience measurement statistics and analyses such as:
  - peaks and troughs in visitor numbers,
  - number and demographic of visitors,

[3] Cf. the section "Privacy implications of intelligent video analytics" below (p. 4).

[4] The Working Group has already dealt with these issues in its Working Paper on Web Tracking and Privacy and Working Paper on the Use of Deep Packet Inspection for Marketing Purposes, available at: http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf .

  - comparison of such metrics across time or other location (e.g., across different branches of a retail store).
- detection of, or prediction of, queues or other bottlenecks,
- workforce optimization.

ADVERTISING and PRICING

- analysis of time spent interacting with advertisements or products,
- customized advertising,
- customized pricing, dynamic discounting, rewards or other benefits and incentives.

SAFETY and SECURITY

- detection of and alarm trigger in case of forgotten, stolen or moved objects,
- breaches of virtual security lines,
- detection of accidents and improper/dangerous conduct[5], and
- detection of mass gatherings, over-crowding, etc.

Intelligent video analytics will use image processing techniques to determine features such as the type of object, movement, direction and speed within frame. This is posed as a question of detection and classification such as “Does this image contain a face?” or “Is this face male or female?” rather than one of identification (i.e. “Is this John Smith?” or “Is this person permitted entry?”). An example of a typical database record from a retail shop equipped with intelligent video analytics would be: date of entry: 12.5.2014, time: 12:02, gender: male, age estimate: 35, camera time: 3s, position: left main entrance. These data can be graphically and analytically processed in order to give the shop manager information on gender and age distribution of shoppers, information on number and frequency of visitors, a shop-floor heat map and other valuable information. Digital displays could be used to deliver targeted ads (e.g., male shaving products if a male visitor was predicted), engage visitors to interact with the ad (e.g., to play games to earn credits or discounts by embedding gesture recognition, touch screens and smartphone integration) or even to entice visitors to connect their behaviour with their loyalty scheme identity.

The scope of possible uses is almost limitless, and practical case–studies range from the charitable to the purely surveillance oriented. A recent example includes an ad campaign showing a bruised woman to raise awareness about domestic violence. Creative use of video analytics was used to clock when people were paying attention to the advertisement, updating a viewer count and slowly altering the image to show the woman gradually healing, sending the message that even attention helps[6]. Other uses of intelligent video analytics may not have such positive connotations[7].

---

[5] For example, detection and safety measures activation in case of an individual falling onto tracks in a metro station.

[6] http://www.oceanoutdoor.com/ocean-news/case-studies/womens-aid-and-ocean-amplify-the-violent-face-of-abuse-with-the-worlds-first-visually-powered-dooh-campaign/

[7] According to media coverage, the smiles of employees at Keihin Electric Express Railway in Japan are tracked by advanced video systems and assessed by computer (http://www.economist.com/node/21553408).

The development of intelligent video analytics is converging with other trends, such as mobile, social, cloud and interactive. Interactions with consumers have become more prominent and multi-channelled with the rapid growth of smartphone usage and new mobile technologies like NFC, beacons and more accurate geo-fencing capabilities. Digital-Out-Of-Home advertising can be combined with location-targeted mobile advertising, using big data to reach the same mobile consumer on larger, higher impact screens and enabling marketers to develop cross-screen, location-based strategies[8]. The growing number of digitally connected screens, more of them being equipped with video and location analytics, will open new privacy challenges in the near future.

Privacy implications of intelligent video analytics

Though individuals are not identified, the implications of intelligent video analytics for privacy, data protection, and other human rights are still significant. Such technologies are employed by law enforcement agencies in order to detect improper or undesired conduct at public places (e.g., sleeping on park benches), to issue warnings for different offences (e.g., play recorded messages to reprimand jaywalking, littering or illegal parking) or even for gender or ethnicity-based decisions. The transfer of control over data from the surveilled to the surveillers, which such systems could represent, may cause a chilling effect and interfere with the right of assembly, prohibition of discrimination and other fundamental rights[9].

Privacy risks exist in the private sector but are perhaps less visible[10]. Individuals have the right to know who is collecting which data about them and for which purposes and in this point in time few of us expect that cameras are able to tell our age, distinguish our gender and track us as we walk around the mall. Some claim that this is creating a one-way-mirror society if consumers are not informed of these practices and do not have the opportunity to control monitoring in retail, public and other spaces or to consent to having their behaviour analysed for marketing and profit[11].

[8] http://www.iab.net/iablog/2015/01/top-5-trends-in-DOOH.html

[9] See Adams, Andrew A. and Ferryman, James M., The Future of Video Analytics for Surveillance and its Ethical Implications (November 12, 2012). Security Journal, Forthcoming. Available at SSRN: http://ssrn.com/abstract=2174255

[10] These may vary from non-intrusive in the case of simple audience counters to medium intrusive gender-based tailored ads spanning towards highly intrusive detection of improper or unlawful activities, purely personalized tailored advertising, creation of black lists, etc.

[11] Dixon, Pam: The One-Way Mirror-Society. Privacy Implications of the new Digital Signage Networks, 2010. Accessible at: http://www.worldprivacyforum.org/wp-content/uploads/2013/01/onewaymirrorsocietyfs.pdf

Industry associations[12] and privacy advocates[13,14,15] have already warned that an appropriate approach to the risks of privacy, data protection and transparency is vital for achieving trust with consumers. Trust is a fundamental precondition for further growth and development of out-of-home advertising, which is currently the main application of video analytics[16]. Furthermore, a 2009 study[17] revealed that 90% of young adults in the USA rejected tailored advertising based on their "off-line" activities. Some provider associations have already taken steps towards self-regulation by adopting codes of conduct[18] and guidelines[19] to respect privacy in out-of-home advertising. They recognized that a proactive and timely approach is necessary in order to avoid regulation imposed by legislators as was the case with the regulation of web-tracking and advertising in EU. There are also examples of regulation on national levels, such as the one in France[20].

The privacy and data protection implications of intelligent video analytics vary according to the level of sophistication and capabilities of such systems. Most papers that deal with these issues distribute particular applications in three categories or levels. Distribution into common categories helps manage the wide array of solutions and privacy implications by looking at commonalities of specific applications. For the purposes of this paper, intelligent video analytics technologies/systems are divided into the following three categories.

---

[12] See Digital Signage Federation: Digital Signage Privacy Standards. Accessible at: 2011, http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002-2011%20%283%29.pdf

[13] See Center for Democracy and Technology (CDT). A Framework for Digital Signage Privacy, 2010. Accessible at: https://www.cdt.org/files/pdfs/A_Framework_for_Digital_Signage_Privacy-Center_for_Democracy_and_Technology-March_2010.pdf

[14] Cf. Information and Privacy Commissioner, Ontario. White Paper: Anonymous Video Analytics (AVA) technology and privacy, 2011. Accessible at: http://www.ipc.on.ca/images/Resources/AVAwhite6.pdf

[15] Cf. Federal Trade Commission (FTC) report Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. Accessible at: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[16] http://www.digitalsignageconnection.com/how-emerging-privacy-issues-could-impact-digital-signage-success

[17] Americans Reject Tailored Advertising. Accessible at: https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf

[18] Cf.: POPAI - THE GLOBAL ASSOCIATION FOR MARKETING AT RETAIL, Digital Signage Group. Best Practices: Recommended Code of Conduct for Consumer Tracking Research, 2010. Accessible at: http://www.popai.com/docs/DS/2010dscc.pdf

[19] Cf.: Digital Signage Federation Privacy Standards: www.DigitalSignageFederation.org

[20] Environmental law "Grenelle II„ (2010-788 of 12 July 2010) gives the French data protection authority (CNIL) the competence to regulate devices used to measure the viewership of advertisements in public places like shopping malls, train stations and airports. Any system that automatically measures the audience of an advertising device or which analyses the typology or behaviour of individuals passing within the vicinity of such advertising device requires prior approval of the CNIL.

Detection. In these cases, the individual is treated simply as an object while his/her personal traits, such as gender or age, are not predicted. Images are not necessarily stored, data is aggregated and advertising use is limited. Individual traits are not collected or processed. Examples include detection of stolen/moved objects, breaches of a secure perimeter, shop-floor heat maps, visitor counters, gesture movement detection and queue-length detection.

Classification. These applications of intelligent video analytics collect and process the detected images in order to predict gender, age or other behavioural information of the individuals, in such a way that the individual would normally not be singled out or identified. Data are used for segment based advertising and customized services, but they are not linked with other data that may allow for identification of the individual (e.g., data from loyalty schemes, smart phone data). Examples include digital signage that detects age and gender and displays segment-specific ads (e.g., for seniors, women in age group 20-30 years, etc.). It must be stressed that as the number of data types related to a specific individual increases, the likelihood of identification also increases as they are more likely to be the only instance of that particular set of attributes. Though identification of the individuals may not be the purpose of this type of processing, segmentation is being applied to individuals, and therefore, as a result of classification, individuals can be treated differently according to the segment they are predicted to belong to. This entails risks of discrimination and stigmatisation (sex or race)[21].

Identification. The purpose of data processing is the identification or singling out of individuals and application of personally customized ads, services or measures. Collected data alone or in connection with other data enables the singling out or identification of the individual. Examples include smart digital signage that identifies the individual, connections with loyalty schemes or social network profiles, biometric face recognition systems, automated number plate recognition systems, etc.

Video analytics resulting in detection and classification constitute processing of personal data and as such require appropriate risk management. Adopting the principle of data minimization by not storing the images, or any unique identifiers derived from image data[22] may assure a more effective protection of rights of the individual. Careful placement of video devices to avoid sensitive areas provides another form of protection[23]. Nevertheless, personal data is still processed during

[21] It is worth emphasizing that, in this connection, the number of classes and the structural richness of collected data may play a role in identifying a person. The boundary between mere detection, classification and identification very much depends, under certain circumstances, on the number of persons “counted” and included in a class. In order to mitigate the risks of identification, only the attributes strictly necessary for the selected classification criterion should be used, and a lower bound on the size of each cluster should be defined.

[22] Some persistence or retention of data, however transient, may in some specific cases be necessary. This may not be the raw image data but some relevant extraction or derivative of the image data needed for comparison purposes.

[23] Federal Trade Commission, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies (2012), https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies , at 13.

the phases of detection and classification, even if only for a short period of time, and implications for the individual may still be present[24].

Recommendations

The Working Group is of the opinion that while intelligent video analytics can provide a number of benefits in various fields such as security, management and advertising, data protection and privacy principles must still be respected.

Lawfulness and fairness

Conditions under which intelligent video analytics may be used should be proportionate to the impact they have on privacy and data protection. Taking into account the commonalities of detection and classification applications, the principle of lawfulness and fairness should be respected principally by adequate transparency mechanisms. Individuals should be fully informed and notified that a system using intelligent video analytics is in place and informed what that means for them in a clear and understandable manner. The use of intelligent video analytics in the public sector, particularly in the case of law enforcement, should in any case be prescribed by law.

Identification applications, where the individual is the object of singling-out or identification, require stricter conditions in order for data processing to be lawful. Lawfulness may be based upon consent of the individual, legal grounds provided for in law or through prior approval procedures in accordance with national legislation. Other approaches such as privacy seals, standards and certification may also be envisaged. Merely providing notice and an opt-out mechanism would likely not be sufficient for identification applications of video analytics due to the level of privacy impact these applications have on the rights of the individual. In addition, different opt-out systems per provider of digital signage would be very user unfriendly. The Working Group strongly encourages providers of interactive billboards to develop user friendly opt-out or consent mechanisms[25].

Particular attention should be paid to the processing of special categories of data, such as data on health and ethnic background, which may lead to discrimination and other negative consequences for individuals. Collection or processing of these types of data by intelligent video analytics solutions should be explicitly avoided. In addition, in order for the processing to be fair, no automated individual decisions should be taken based on evaluations of behaviour or conduct as analysed by intelligent video analytics systems (especially in case of profiling based on sensitive personal data, such as race or health). Such decisions at least require human intervention.

---

[24] A clear example would be the case of false segmentation – an individual mistakenly treated as male (or vice versa) and shown a gender-specific or even ethnicity-based ad. Other implications could be envisaged for example an individual being mistakenly identified as being drunk in public, trespassing or supposedly stealing.

[25] Cf. Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Transparency

Individuals should be adequately informed about the use of intelligent video analytics. It is quite reasonable to expect that the individual would want to know when, where, by whom and for what purposes data about his/her gender, age and movements are being collected and processed. Individuals should know whether they are being subjected to "ordinary" CCTV that merely stores images or whether the system is able to track their movement, assess their behaviour or measure their attention span to specific digital billboards. As was already stressed, the issue of transparency was already identified by various stakeholders as one of the main preconditions for achieving trust and assuring future growth and development of intelligent video analytics solution, particularly in the field of digital-out-of-home advertising and digital signage[26]. Non–transparent applications[27] could severely undermine user trust, and deter growth and development.

In order to ensure that individuals are fully informed the Working Group recommends that organisations adopt a layered approach to achieve an adequate level of transparency. Such an approach will deliver key information at the point of collection and may be supported by more in-depth information through various channels including nearby posters, leaflets and website information.

At the point of data collection, consumers should be given clear, prominent notice of which devices will process their personal data such that the individual can be certain they are aware of the physical location in which the device(s) operates. To the extent possible, the notice should appear noticeably close to each device that is collecting the information (one notice should not cover, for example, an entire shopping mall or an airport terminal). Existing notices describing the operation of CCTV would not be sufficient without modification and the use of unmarked or hidden devices/sensors should not be allowed. The development of common pictographic standards and notices may be foreseen in the future which could enable a simpler and better recognition for the users.

The notice should provide the following information:

- the purpose of the device/system,
- information on the identity of the data controller,
- information on data being collected,
- users of collected data,
- information whether data are combined with other data,
- where further information and details may be obtained.

---

[26] http://www.digitalsignageconnection.com/how-emerging-privacy-issues-could-impact-digital-signage-success

[27] An example of an inappropriate approach is the one of motor oil personalized digital sign campaign in London. As cars approached the digital billboard, images of motorists' license plates were captured and matched to a database of vehicles. The billboard then displayed an ad tailored to that make and model of car. The campaign was quickly cancelled due to questions of transparency and lawfulness.

In order to be fully transparent and fair, the notice should also provide relevant reassurances (such as information that images, or any unique identifiers derived from image data are not stored and that data is not combined with other sources).

Finally, in-depth information about the system should be made easily accessible to individuals for example via a web published privacy policy, by telephone or through on-site information desks.

Proportionality (*data minimization and retention)*

In order to respect the principle of proportionality, the concept of privacy by design should be followed. Operators of intelligent video analytic systems should conduct privacy impact assessments in order to identify the risks and relevant safeguards in a timely manner. Immediate deletion of images, or any unique identifiers derived from image data, real-time anonymization of collected data and deletion of historical raw data may significantly reduce the risks.

In addition, operators should consider whether the purpose of the processing really necessitates non-stop analysis, or whether limitations in time and geography would allow achieving the same purposes. For example, the application may be limited to business opening hours and working days, and time-lapse may be considered (measuring every other day or week, or other types of sampling). Last but not least, operators should take into account that video analytics may be prohibited in places such as saunas, swimming pools, places of worship and hospitals.

Purpose specification - finality

Respect for the principle of finality may be achieved by proper notices and accountability measures that limit the uses of collected data. Data should not be used for purposes that were not explicitly specified and made known to the individuals. There is a real risk that data collected for certain purposes, such as management or security, may be used for other essentially incompatible purposes, such as marketing or surveillance purposes. There is also a real risk that data may be used for new purposes (something known as 'function creep'), unknown to the individuals, with new, unforeseen data protection risks.

Data quality

The issue of data quality is of particular importance in this respect. Issues of data accuracy and data being up to date should be precisely analysed during privacy impact assessments and different fall-back and other mechanisms should be foreseen.

It must be noted that all applications of intelligent video analytics operate within certain margins of accuracy and may as such result in less than accurate detection of individuals, objects and movements. The consequences of an inaccurate prediction will depend on the purpose of video analytics system. This is of particular importance whenever intelligent video analytics is deployed in the public sector, particularly when used by law enforcement agencies (e.g., detection of un-

usual movement or behaviour in public places). Accuracy issues may have severe consequences for the individual in this case[28].

Data security

Appropriate measures and procedures should be employed in order to ensure that data are secured from unauthorized access, alteration or destruction. Particular attention should be paid to identification and mitigation of the privacy risks that are associated with the use of anonymization techniques[29]. This again should be considered when determining the purposes and scope of data collected during the privacy impact assessment.

Rights of the individual

Detection and classification tasks do not require the storage of the processed images, or any unique identifiers derived from image data, but operate with aggregated data and statistics. Hence the data do not refer to the individual. Identification applications are of course significantly different. In these cases, the right to access one's own data and the rights of rectification, correction or deletion of unlawfully collected or false data play an important role, e.g. in video analytics systems that involve facial recognition, number plate recognition, personalized advertising and other technologies.

[28] The same may apply also in private sector (for example in the case of video detection of license plates and creation of black lists of drivers, e.g., by gas stations).

[29] Cf. for example Article 29 Working Party Opinion on anonymization techniques, accessible at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

About the International Working Group on Data Protection in Telecommunications ("Berlin Group")

The International Working Group on Data Protection in Telecommunications (IWGDPT, a.k.a. "Berlin Group") includes representatives from Data Protection Authorities and international organisations dealing with privacy matters from all over the world. It was founded in 1983 in the framework of the International Conference of Data Protection and Privacy Commissioners at the initiative of the Berlin Commissioner for Data Protection, who has since then been chairing the Group. The Group has since 1983 adopted numerous recommendations ("Common Positions" and "Working Papers") aimed at improving the protection of privacy in telecommunications. Since the beginning of the 90s the Group has in particular focused on the protection of privacy on the Internet. More information about the Work of the Group and the documents adopted by the Group are available for download on the website of the Group at http://www.berlin-privacy-group.org .