IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 18, 2019, accepted August 4, 2019, date of publication August 9, 2019, date of current version August 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2934226

Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective

MAMOONA N. ASGHAR[1,2], NADIA KANWAL[1,3], BRIAN LEE[1], MARTIN FLEURY[4], MARCO HERBST[5], AND YUANSONG QIAO[1]

[1]Software Research Institute, Athlone Institute of Technology, Athlone, N37 HD68 Ireland
[2]Department of Computer Science and IT, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
[3]Department of Computer Science, Lahore College for Women University, Lahore 54000, Pakistan
[4]School of Science, Technology and Engineering, University of Suffolk, Ipswich IP4 1QJ, U.K.
[5]Evercam Ltd., Dublin 1, Ireland

Corresponding author: Mamoona N. Asghar (masghar@ait.ie)

This work was supported in part by the Marie Skłodowska-Curie (MSC) Career-FIT Postdoc Fellowship (Project ID: MF 2018-0179) funded by the European Union's Horizon2020 Research and Innovation Programme under the MSC under Grant 713654, in part by the Science Foundation Ireland (SFI) under Grant SFI 16/RC/3918, and in part by the European Regional Development Fund.

ABSTRACT From an individual's perspective, technological advancement has merits and demerits. Video captured by surveillance cameras while a person goes about their daily life may improve their personal safety but the images collected may also represent an invasion of their privacy. Because of the ease of digital information sharing, there exists a need to protect that visual information from illegal utilization by untrusted parties. The European parliament has ratified the General Data Protection Regulation (GDPR), which has been effective since May 2018 with a view to ensuring the privacy of European Union (EU) citizens' and visitors' personal data. The regulation has introduced data safeguards through Pseudonymisation, Encryption, and Data protection-by-design. However, the regulation does not assist with technical and implementation procedures, such as video redaction, to establish those safeguards. This paper refers to the GDPR term "personal data" as "visual personal data" and aims to discuss regulatory safeguards of visual privacy, such as reversible protection, from the technological point-of-view. In the context of GDPR, the roles of machine learning (i.e. within computer vision), image processing, cryptography, and blockchain are explored as a way of deploying Data Protection-by-Design solutions for visual surveillance data. The paper surveys the existing market-based data protection solutions and provides suggestions for the development of GDPR-compliant Data Protection-by-Design video surveillance systems. The paper is also relevant for those entities interacting with EU citizens from outside the EU and for those regions not currently covered by such regulation that may soon implement similar provisions.

INDEX TERMS Blockchain, CCTV, cryptography, data protection-by-design, gdpr, pseudonymisation, reversible protection, visual privacy, video redaction.

I. INTRODUCTION

As technology advances, the ways of collecting and processing personal data are now almost completely digitized. Companies are established to collect and process the identifiable personal data of their customers [1]. Banks, collect the most confidential financial details of individuals. However, there are many other entities that have access to personal data, amongst which are: communication providers for broadband, landline, television, and mobile services; insurance companies; retail shops; and utility providers for electricity, gas, and water services. Companies frequently collect this information, ostensibly to ensure a better customer experience. Customers may often trust them by providing this information without a second thought and without bothering to even ask how this identifiable data is processed by a company. Many people are aware that those companies may have complete and identifiable personal data information (such as their name, home address, credit/debit card numbers, bank details, and other service-specific information). However, beyond those companies, there are some service providers who covertly monitor the day-to-day activities of people and process their personal data. These are security companies, which monitor people, often using surveillance cameras for

The associate editor coordinating the review of this article and approving it for publication was Feng Shao.

the purpose of safety. Visual surveillance is the principal context of the current paper.

Security is an overarching concept that is also tied to an individual's personal data security. It is not simply the security offered to companies, other organizations, and state players as a service to protect their interests. For an individual, during each working day, the thought of being safe starts at the time of leaving home and ends on the return home. Video surveillance cameras, such as those that are part of a Closed Circuit Television (CCTV) system, are utilized as safety tools by recording individuals' activities. People are very much exposed through video surveillance in the name of safety or security. Examples of video surveillance applications include: the monitoring of sensitive locations (such as embassies, airports, nuclear plants, military zones, and at border controls), intrusion detection (residential and retail monitoring); public safety installations (such as for traffic control, and at car parks and ATM machines); vehicle detection systems through license plate recognition; event detection (such as during child care and the care of the elderly); and marketing and statistics-gathering systems (such as for discovering customers' habits and behaviours, and recording the number of visitors). Illicit activities such as theft, assault, and shooting incidents are captured by the widespread deployment of surveillance cameras, which clearly benefits the majority of citizens. Nevertheless, with the advent of enhanced CCTV based security, more challenges are presented in terms of people's privacy protection, and their dignity and free will, even when they are being monitored.

The invasion of privacy, due to the extensive use of surveillance cameras, has been widely and frequently reported. Particularly in the UK, some may say that there is an excessive number of CCTV cameras. For example, any citizen, as a daily average in London, is caught on about 300 CCTV cameras [2]. In fact, there are about 4 million CCTV cameras in the country as a whole. In respect to the abuse and misuse of surveillance data, there are reports [3] of various disturbing incidents. In 2005, according to the British Broadcasting Corporation (BBC) news [4], a woman in Liverpool was spied on by four council workers misusing a street CCTV pan-tilt-zoom camera. The extremely intrusive use of CCTV surveillance by Nahid Akbar (in 2017) [6] in her neighbourhood was penalised by the Scottish court. The Scottish court found that Ms. Akbar was in breach of the fifth Principle of Data Protection, resulting in the £17,000 damages awarded to the affected Mr. and Mrs. Wooley. Outside the UK, an instance of illegal spying on celebrities and government officials occurred [5] when a museum's CCTV camera was misused by a security guard to spy on the Chancellor of Germany's (Angela Merkel's) private flat. Such incidents can occur in numerous sensitive situations: such as when people are identified in surveillance video captured during a demonstration or rally, or when, in oppressive regimes, political opponents active against a sitting government can be threatened or harmed later.

The following quotation of Benjamin Franklin is well suited to today's secure society:

"Any society that will give up a little liberty to gain a little security will deserve neither and lose both."

In response, it may be said that the European Union (EU) parliament has introduced a General Data Protection Regulation (GDPR) [7] into European law in respect to the protection of individuals' rights to freedom, while their personal data, in the form of texts, audio, and videos, are processed. GDPR seeks to ensure data protection and privacy during the processing of personal data of all individuals within the EU and the European Economic Area (EEA). GDPR also covers the transfer of personal data outside the EU and EEA area. In GDPR law, the data subject (GDPR term for a natural person/individual) has complete control over the processing of their personal data. Without the consent of the data subject, the data cannot be processed and exported outside the EU. GDPR provides extensive guidelines to data collectors and processors in order to maintain the confidentiality of the data subject's information. The law covers the rights of individuals and instructs data controllers and supervisory authorities accordingly. If personal data collection companies do not provide GDPR-compliant solutions for their data subjects (customers and employees), heavy penalties could well result. A survey [8] shows that 80% of businesses in Europe know minimal details or almost nothing about the implementation of GDPR within their companies. In fact, GDPR is a global data protection regime, which according to the authors' analysis can be summarized as:

- **Harmonization** of privacy protection regulation in the EU.
- **Freedom rights** for EU citizens/visitors by providing safeguards for their identifiable data.
- **Notification:** Meaningful symbols must be placed by controllers/processors to notify people whenever CCTV recording is in progress.
- **Access rights of individuals:** Personal data should be collected by initiating a consent form. The regulation gives the right to individuals to gain access and request the erasure of their personal visual data in a reasonable time-frame.
- **Privacy Safeguards:** Data should not be stored and exported openly; there should be privacy safeguards to hide the originality and identification of data through automated techniques.
- **Retention Period:** Personal visual data should be kept for a specific time-frame.

This paper overviews the relevant articles within the first four chapters of the GDPR regulation (see Section II.A) in terms of re-defining the concepts of personal data, pseudonymisation, encryption and Data Protection-by-Design in accordance with the visual protection of data subjects. Thus, the following research questions are posed for a GDPR-compliant video surveillance industry:

TABLE 1. GDPR descriptions for data and the authors' definitions for visual data.

Terms	GDPR Descriptions	Relevance for Surveillance Companies
Data	The term is used collectively for automated or manual raw/processed information.	Recorded videos
Personal data	Data related to a living person who is or can be identified directly from the given data or in combination with other available information.	▪ **Current biographical status:** name, Date-of-Birth (DoB), home & work address, phone, email address, and social security number ▪ **Appearance and behavior**: Skin color, eye color, weight, identification marks, and character traits. ▪ **Job and education related data:** salary, tax no., employee id and student id.
Automated data	The digitized form of data i.e. recorded information is processed through computer/devices.	Individuals captured and recorded through camera devices and the IP addresses of devices.
Manual data	The information taken and kept as a part of a related filing system for the maintenance of records.	Manually taken (recording of) person's information, e.g. name, address, workplace, email address, phone no. These data are more specific to employees and customers of the surveillance company.
Genetic Data	The form of personal data that is taken through the analysis of biological samples of an individual.	This form of data is kept for a company's employees. It is irrelevant for people monitored outside the companies.
Biometric Data	The form of data produced from some technical processing relating to the physical, physiological or behavioral characteristics for the unique identification of an individual, e.g., through face recognition in images or dactyloscopic data (such as fingerprints).	Analysis of captured images for a specific person, i.e. to find ethnic origins through looks and traits.
Sensitive personal data	The data related to an individual's ethnic origins, religious beliefs, political opinions, sexual life, mental or physical health, criminal convictions or the alleged commission of an offence, trade union membership and so on.	Analysis of captured images for specific person, e.g. to find ethnic originc, physical health through looks, gait and other traits. The individual has some additional rights during processing of his/her sensitive data.

Q1: What is the visual personal data of the data subject? (Descriptions of data relevant to visual data are given in Table 1 and Section III describes visual data).

Q2: Do all recorded visual data need to be protected? (Section II (specifically II.A))

Q3: In what circumstances are GDPR-compliant surveillance cameras required? (Section III.A)

Q4: What are the pseudonymisation vs. anonymisation strategies for visual data protection? (Section IV.A)

Q5: What is Data Protection-by-Design in respect to video surveillance companies? (Sections IV and V)

The purpose of this paper is to clarify the aforementioned questions with the following contributory points:

- Brief overview of the GDPR relevant articles requiring clarification for visual data collection companies/controllers/processors.
- The role of technology in the implementation of Data Protection-by-Design solutions for CCTV data besides the implementation of policies.
- A review of the existing solutions for GDPR-compliant video-redaction methods for surveillance applications; and
- Forthcoming real-time technologies for implementing Data Protection-by-Design solutions.

The remainder of the paper is organized as follows. Section II is an overview of the pertinent articles of the GDPR regulation. That section provides a clear picture of GDPR for the CCTV surveillance industry, along with GDPR safeguards and distinguishable concepts of pseudonymisation vs. anonymisation. Section III presents identifiable visual personal data, identified premises and use-cases for mandatory GDPR-compliant surveillance. Section IV discusses the role of technology in GDPR-compliant Data Protection-by-Design solutions with market-based solutions. Section V presents future Data Protection-by-Design solutions by incorporating other technologies and finally, Section V1 concludes the paper with several observations and comments.

II. GENERAL DATA PROTECTION REGULATION

The Data Protection Directive 95/46/EC (Directive 95/46/EC, 1995) was introduced in October 1995 by the EU and came into force in December 1995. The purpose of this directive was to protect the individual's personal data. The directive was implemented in October 1998 as an important part of EU privacy and human rights law. That directive was superseded with the European General Data Protection Regulation (GDPR), adopted in April 2016 and becoming enforceable on May 25, 2018 in all EU member states. The aim of GDPR is to harmonize the degree of data protection across the EU countries. By introducing a single law across all EU states, the intention was that it will bring better transparency to the processing of an individual's data and boost the collective digital economy of the 28 participating EU states (possibly 27 states if the UK leaves the EU). Personal data-collecting organizations in these EU countries, will probably be most affected by the GDPR.

Data protection, as defined by the Joe Meade (Ireland's Data Protection Commissioner) [9] is as follows:

"Personal data protection applies to all our interactions with public and private sector organizations and thus applies to applications, purchases and transactions in State services, business and economic matters, in the social and medical areas, in the workplace and in the globalized technological arena."

The Data Protection Acts 1988 and 2003 confer rights onto individuals and place responsibilities on the shoulders of those who process personal data. GDPR applies globally; thus companies outside the EU processing personal data of an EU citizen with the aim of providing services, selling goods or monitoring the behavior of any EU citizen, e.g. any video surveillance companies [10] or health centers, are bound to the regulation. A Data Protection Officer (DPO) should be appointed by these companies. The appointed DPO will be in charge of the GDPR compliance of that organization. The stakes have been set high, as failure to comply will result in a substantial fine of 4% of the company's global revenue or of 20 million Euros, whichever is higher. Due to the recent misuse of Facebook's customer data [11], all eyes are on the proper protection of customers' private information.

The resulting harmonization in law makes it easier for EU citizens to understand how their data is being used and how they can raise complaints, even if they are not located in an EU member country. GDPR is not applied to IT-related data alone; it has broad-sweeping implications for a whole company, such as for the handling of sales, marketing and human resourced data.

A. OVERVIEW OF FOCUSED GDPR ARTICLES

The EU GDPR aims to increase the privacy of the EU's citizens and allows regulatory authorities to use maximum powers to take actions against any businesses/companies that breach the law. The regulation (GDPR) has 173 recitals (representing GDPR goals), and 11 chapters which cover 99 articles [7]. However, for the implementation of GDPR-compliant surveillance systems, the first four chapters cover all necessary articles for secure processing of personal data by the controllers/processors. For the ease of readers, a flowchart of focussed GDPR articles in this paper is presented in Fig. 1.

Notice that as the main focus of this paper is technological aspects of GDPR. Though the authors have applied due care and consideration to legal aspects of GDPR, readers should bear in mind the technological focus and perform due diligence in respect to any legal aspects, which are added for the reader's convenience and are not intended to be legally definitive.

1) GDPR DESCRIPTION and DEFINITIONS

Article 4 of GDPR [7] covers the definitions of terms used throughout the regulation. Table 1 defines the term data. For CCTV controllers, this current paper also discusses some other important definitions to clarify the concepts. Overall, GDPR considers seven types for the term 'data' throughout the regulation and all are relevant for surveillance data collection companies. However, notice that according to GDPR (article 9) "Genetic Data" and "Biometric Data" are included in the 'sensitive' data definition or equally "special categories' of personal data definition. Thus, in terms of GDPR definitions, as opposed to descriptions, "Genetic Data" and "Biometric Data" appear together in the same definitions.

2) GDPR PRINCIPLES & LAWFULNESS OF PROCESSING

Article 5, clause-1 describes six (6) GDPR principles, that is lettered a–f, for ensuring privacy during processing of personal data.

[Art. 5-1(a)] Lawfulness, fairness and transparency

Lawfulness: Processing must be in accordance with the GDPR criteria.

Fairness: Personal data should be processed in ways that the subjects would reasonably expect and not use it in ways that have unjustified adverse effects on them.

Transparency: Explicit reasons for the collection and processing of personal data are required.

[Art. 5-1(b)] Purpose limitations

Personal data can only be obtained for *"specified, explicit and legitimate purposes"*. The data subject must be aware of the reason for collecting data. There should not be any processing without further consent, although, the data related to public interest, research or statistical purposes have no obligations in respect to purpose limitation.

[Art. 5-1(c)] Data minimisation

Data collected specific to a subject should be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*, which means that the minimum amount of data should be collected and retained for specific processing.

[Art. 5-1(d)] Accuracy

The collected data must be *"accurate and where necessary kept up to date"*. There should not be any alterations by

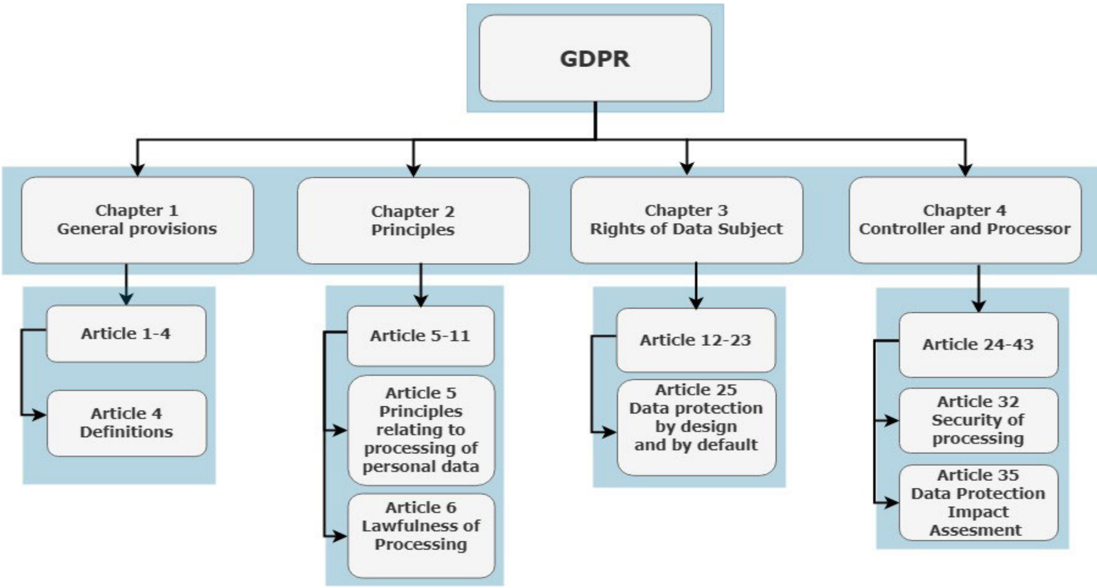

FIGURE 1. **Flowchart of reviewed GDPR Articles.**

way of ensuring good protection against identity theft. Data controllers must build editable data management systems to allow the subject to update their data.

[Art. 5-1(e)] Storage limitations

The regulator expects that personal data are *"kept in a form which permits identification of data subjects for no longer than necessary"*. With proper safeguards, data related to public interest, research or statistical purposes can be stored for a long time. The data that are no longer required should be erased/deleted from the repositories of a controller.

[Art. 5-1(f)] Integrity and confidentiality

During processing, the collected data must maintain its integrity and confidentiality. The controllers should use appropriate technical or organizational measures to provide *"appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage"*.

[Art. 5-2] Accountability

Controllers shall be accountable if the data processing is not compliant with clause 5.1(a-f) principles.

Article 6 concerns the lawfulness of processing by providing a proper "consent form" for the data subject for the processing of their personal data. The processing should be done while keeping the legal obligations in mind. Article 6 (4)(e) mentions the appropriate safeguards for personal data by using the procedures of encryption or pseudonymisation (Section II.C). Article 6(f) clarifies that legitimate processing of data by the controllers is allowed, except that this processing should not override the rights and freedom of the data subject, especially if the data subject is a child.

Article 7 is about the conditions for getting consent about the processing of personal data from the subject. Articles 8 to 10 discuss the processing of personal data related to children, special categories and criminal convictions and offences, which are out of the scope of this paper. Article 11 indicates that if the controller is processing personal data, which do no longer identify that particular data subject, then the controller is no longer compliant with the GDPR.

3) RIGHTS OF THE DATA SUBJECT

Chapter III-GDPR is an important chapter, which demands a proper focus from all companies dealing with the processing of personal data. This is a detailed chapter with five subsections. Section 1, Article 12 transcribes the transparency and modalities of the rights of data subjects. Section 2, including Articles 13-15, is about information and access to personal data. Article 13 deals with the information that should be provided to the data subject when their personal data is being acquired or processed. Article 13(2) defines the additional information provided by the controller to the data subject regarding personal data retention time, the right to request an erasure of personal data, withdraw consent, the right to lodge a complaint with the supervisory authority, the statutory or contractual requirements, and the existence of automated decision making for profiling. Article 14 is about personal data that has not been directly obtained from the data subject. Article 15 has information about the right of access by the data subject. The controller should provide a copy of the personal data undergoing processing, which shall not adversely affect the rights of freedom of others. Section 3 ranging from Articles 16 to 20 are fundamentals that should be known by EU citizens. Articles 16 to 18 are about their rights of rectification, erasure, and restrictions on the processing of their personal data. In short, the following eight (8) rights are given to data subjects under the umbrella of GDPR:

1. ***Right to access*** (Article 15): Data subjects have the right to request access to their collected personal data

and can inquire of a company about the use of their data. The company is bound to provide a cost free copy of personal data in an electronic format upon request.
2. ***Right to rectification*** (Article 16): This ensures that individuals can have their data updated, in case of changes and if the data are incomplete or incorrect.
3. ***Right to erasure*** (Article 17): Data collection companies must delete the data of subjects if they are no longer their customers, or if they withdraw their consent from a company to use their personal data.
4. ***Right to restrict processing*** (Article 18): Individuals can request that their data should not be used for processing. Their record can remain in place, without any use.
5. ***Right to be informed*** (Article 19): This specifies that before collection of any data by companies, individuals must be informed. Consumers have to opt in for their data to be collected, and consent must be freely given rather than implied.
6. ***Right to data portability*** (Article 20): Individuals have a right to transfer their data from one service provider to another.
7. ***Right to object*** and stop the processing of their data for direct marketing (Article 21).
8. ***Right to be notified*** within 72 hours of a data breach (Article 34).

4) GDPR PRIVACY PRINCIPLES

Article 25 describes the key *privacy principle* for all businesses, i.e. Data Protection-by-Design and –by-default. This article serves as the backbone for GDPR-compliant businesses by implementing privacy protection for the sensitive data of a subject.

- **Data Protection-by-Design:** This means that *"appropriate organizational and technical measures to ensure personal data security and privacy are embedded into the complete lifecycle of an organization's products, services, applications, and business and technical procedures"*. The proposed technical measures are pseudonymisation and data minimization.
- **Data Protection-by-Default:** This means that: (i) only necessary personal data are collected, stored, or processed; and (ii) personal data are not accessible by un-authorized people.
- **Certification:** Compliance with Data Protection-by-Design and -by-Default requirements should be demonstrated through an approved certification (as stated in Article 42).

5) SECURITY OF PROCESSING

Article 32 is an important article in respect to providing secure processing for personal data. This article emphasizes that the controller and processors should implement appropriate technical and organizational measures to ensure an appropriate level of security to preserve the rights and freedoms of a data subject. Article 32(1) describes the following security measures:

(a) Pseudonymisation and encryption of personal data.
(b) Ensuring the procedures apply across the range of security services i.e. *"confidentiality, integrity, availability and resilience"*.
(c) In the event of an emergency, quickly restoring the availability and access to personal data.
(d) Ensuring the regular evaluation and validation testing of the adopted security procedures for effective privacy protection.

Article 32(2) points out the risks for processing, i.e. accidental and unlawful destruction, loss, alteration, unauthorized disclosure of processed and stored data. These risks should also be assessed along with assessment of the appropriateness of security levels.

6) DATA PROTECTION IMPACT ASSESSMENT

Article 35 describes the procedure of Data Protection Impact Assessment (*DPIS*), whereby, if processing is done automatically through technologically-advanced means, then a DPIS should be performed. DPIS should be carried out by the controller upon the advice of a designated Data Protection Officer (DPO). DPIS must be performed on the automated procedures, i.e. profiling in which legal impacts upon a data subject are assessed, whether there exists a special category of data or personal data relating to the criminal convictions and offences. DPIS must contain a systematic description of the envisaged processing operation in a legitimate way. The assessment of the risks to the rights and freedoms of data subjects should be given. The measures to address the risks, i.e. safeguards, security measures and mechanisms to ensure the protection of personal data in compliance with the regulation should also be present in the DPIS. Article 36 is about prior consultation of controllers with the supervisory authority prior to the DPIS under Article 35, if processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Article 37 ensures the designation of a DPO with professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred in Article 39. Article 37(2) facilitates that by stating that, for this group of undertakings, controllers may appoint a vigilant and constantly available DPO. A DPO can also be a staff member of a controller's team. Articles 38 and 39 describe the position and duties of a DPO in detail.

B. GDPR SAFEGUARDS

From the previous section's overview of GDPR, it can be clearly perceived that EU citizens have control over their personal data and without their will, companies cannot collect and process their personal information. GDPR relaxes the controllers/processors' need to retain the personal data of the subject by providing safeguards in the form of pseudonymised information and/or encryption.

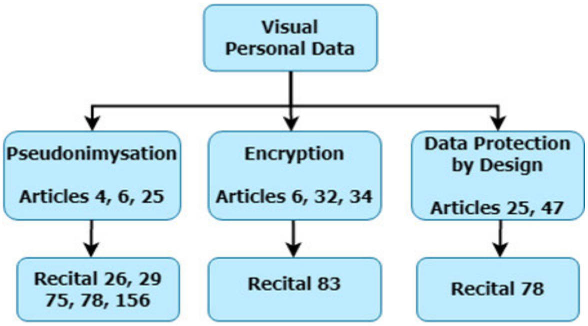

FIGURE 2. Safeguards designated by GDPR.

(Article 6(4) (e) and Article 32(1) (a)). Recitals 26, 78 clarify the processes of pseudonymisation. Recital 83 explains that encryption should not be weak and should ensure confidentiality. The regulation just uses the terms but does not assist with technologies, methods and technical information for Data Protection-by-Design. This current paper now provides an insight into GDPR-compliant technical solutions for confidential video redaction of data subjects of that video. To facilitate reading, the targeted terms from GDPR are presented in Fig. 2.

C. PSEUDONYMISATION VS. ANONYMISATION

GDPR came into force in May 2018, with the result that surveillance-data collection companies now must understand the main terms, as well as the procedures, needed to be adopted according to the regulation. However, the following two safeguard terms are still somewhat ambiguous and might be used interchangeably. All the same, these two terms are clearly different and, hence, need to be understood so as to provide GDPR-compliant safeguards for the captured visual personal data of a subject.

Anonymisation: is the safeguarding of data by adopting an irreversible automated method. The term irreversible is important to understand, as the anonymous data cannot be reverted back to its original form or cannot be used for the identification of the data subject by deploying any practical methods.

Pseudonymisation: is the safeguarding of data by replacing the actual personal information with a pseudonym through an automated method, so that the data subject cannot be directly accessible through a pseudonym.

The previous definitions indicate a distinction between anonymized and pseudonymised data. The distinguishable definition by the Data Protection Commission [12] of Ireland is as follows:

"Although pseudonymisation has many uses, it should be distinguished from anonymisation, as it only provides a limited protection for the identity of data subjects in many cases as it still allows identification using indirect means. Where a pseudonym is used, it is often possible to identify the data subject by analysing the underlying or related data."

The above pseudonymisation definition shows that the data can be reversible/identified in some cases. Here, the term reversible shows that the data subject can be recognized by using any other related information or automated method even when the data is not converted back to its original form. So, in general, one can distinguish both terms by saying that: pseudonymisation can be a safeguarding technique that may be reversible but anonymisation is an irreversible technique to provide protection to data. Irreversible anonymised data is out of the scope of the regulation [13] and controllers can keep this form of data for an indefinite period of time (for future statistical analysis) without any compliance issues arising with the GDPR.

Now the question arises that if the controllers retain the anonymised form of data, then what would be the purpose of retaining that data? Controllers cannot revert the data back to its actual form for any kind of processing, even if it was legal. Hence, it may be considered merely wasteful of storage space at the CCTV controllers end to keep this form of data which is meant for future statistical analysis, should that processing at some distant, future date be permissible, even though currently it is not permissible.

This scenario might be like a scenario in which somebody locks a data file in an unbreakable box and throws the lock's key into the river. Consequently, now the file (in a box) becomes a life-long secret and cannot be taken out by any means, even for a useful purpose. To avoid that situation, as anonymized data evidently has potential beneficial uses, such as the analysis of correlations between the health status and the condition of patients, another solution might be possible, as now described:

If the box's opening key is hidden separately and can feasibly be eventually (at some distant, future date in time) used by controllers to open the box then this procedure is called pseudonymisation and the file is still considered to be personal data, and, hence, needs to be compliant with the GDPR.

The GDPR emphasizes pseudonymisation OR encryption (Article 6(4)(e)) and pseudonymisation AND encryption (Article 32(1)(a)). In Article 6, the use of the word OR in between these two procedures and in Article 32, the use of the word AND are important and, thus, are highlighted in this current paper. Controllers may consider that these two procedures are equally appropriate as a means of securing video personal data. However, it is worth mentioning that encryption is always reversible but that pseudonymisation can be or cannot be. Although encryption and pseudonymisation can be used simultaneously or separately, they are not alternatives to each other that can be assessed according to their merits and demerits.

III. RECOGNITION OF VISUAL DATA

In videos, personal data are the person's physical information and their behaviour. Physical information includes looks, clothing information, skin, eye, hair color, health and so on, while behavior includes gait, physical actions, and facial

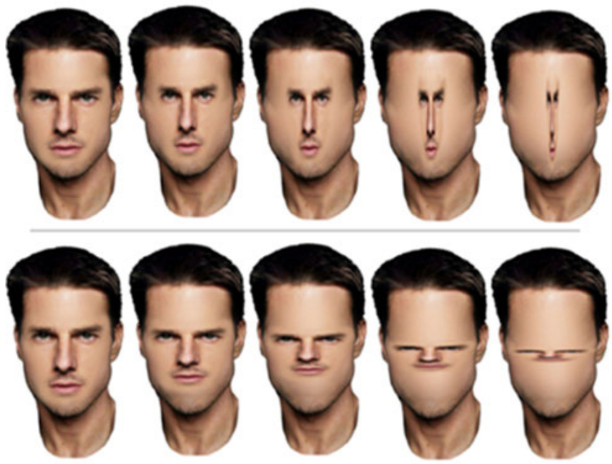

FIGURE 3. Obscuring of faces for non-identification of person (Gilad-Gutnick *et al.*, 2018).

gestures. The recognition of humans through faces, clothes, gaits, and actions within surveillance videos is not difficult for a normal human. Interesting research on facial recognition [14] was performed by MIT neuroscientists. This revealed that humans are remarkably good at recognizing faces even if they are highly distorted. That paper [14] includes numerous experiments to significantly deform faces by horizontal and vertical compression (also known as thinning and flattening). Gilad-Gutnick *et al.* [14] found that people are very good at recognizing thinned and flattened celebrity faces. In fact, a thinning or flattening of as much as 80% has almost zero impact on recognition accuracy. Beyond 80%, performance starts to fall off but even at a distortion level of 90% – in which the face is reduced to a mere 'sliver' – volunteers were still able to recognize about half of the celebrities. After those experiments, Gilad-Gutnick *et al.* wanted to know which parts of the face were most important in terms of recognition. This led them to create some – well – amusing stimuli. They performed selective compression of the 'internal features' of Tom Cruise's face, while the 'external features' are left untouched (Fig. 3). Gilad-Gutnick *et al.* interpret this finding as suggesting that vertical 'within-axis distance ratios' are key to facial recognition. If one compresses the whole face, the relative distances between the eyes, nose, and hairline do not change. However, if one only compresses the internal features, these ratios are altered.

There are some studies in which people are detected and recognized through gaits. Bouchrika and Nixon [15] detected and recognized people through their gaits by using shape-based feature correspondence between consecutive frames. They derived a gait signature by means of a model-based method, with the result that their system was 92% successful in recognizing people. In another example, Semwal *et al.* [16] presented periodic cellular automata rules for different gait state classification and prediction through Extreme Machine Learning (EML). They formulated sixteen rules for cellular automata and eight rules for each human leg, achieving 60% accuracy in prediction during their experiments.

A. PREMISES FOR GDPR-COMPLIANT SURVEILLANCE

As the previous discussion indicates, facial and gait recognition are easy tasks for a normal human. Therefore, privacy protection should be affected through methods in which a sufficient level of distortion is applied across the whole of a video. This section describes the boundaries/premises whereby GDPR compliance is achieved when installing surveillance cameras.

1) PERSONAL SPACE VISUAL DATA

Personal recorded data occur in a domestic setting or within a household, as per Article 8 of the European Convention on Human Rights [17] and, hence, is within the personal space of visual data. For example, suppose that a CCTV system is installed in one's home, such as in a living room or in a bedroom for monitoring an elderly person for safety purposes, or in a playground for monitoring a child, again for safety purposes. It could also be installed in a garage for vehicle safety and in other similar circumstances. Video footages obtained in those scenarios are not required to be protected, as they are not forwarded to any third person, unless, that is, a serious incident related to theft, any damage to property, or a health issue related to a child or elderly person occurs and is captured by a camera. Thus, these CCTV footages, in general, do not have a value for local authorities, city planners or other third parties. Such footages can be called 'private data' and GDPR compliance is then not mandatory for such domestic usage.

2) IMPERSONAL SPACE VISUAL DATA

Impersonal space data is not linked to an individual and, being unsuitable, cannot be used for surveillance and control purposes. Examples of such data are the monitoring of traffic flows within public transport, shopping malls, crowds in roads/public parks, and construction sites and for the purposes of sports and event management. Usually public authorities collect this data by means of infrared video or by CCTV. Such data may not be automatically considered as sensitive, as it does not measure individuals but rather flows of vehicles or impersonal crowds. Similarly, impersonal data for surveillance purposes comes from the aggregation and combination of survey and registration data in a city [18]. Such kinds of data may also be known as Public data. In this setting, GDPR-compliant CCTV cameras are not necessary but the protection of recorded videos from misuse is definitely essential.

3) PROTECTED SPACE VISUAL DATA

Another important space lies in a category lying between Private and Public spaces. This is the semi-personal-impersonal space, and, herein, it is called 'protected space'. Fig. 4 clarifies the concept of protected space. People usually install cameras for their safety in protected spaces, e.g. in gardens

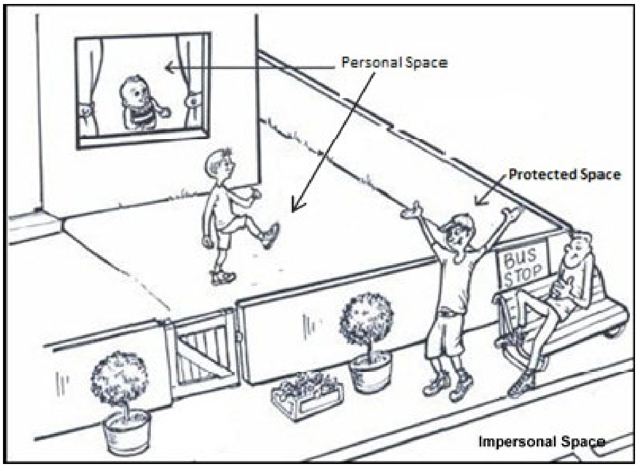

FIGURE 4. Concept of Premises for CCTV monitoring, after [19].

or out of doors (for an external viewpoint). The following are some identified protected spaces:

i. Outside road view from a home/office.
ii. Outside footpaths/walkways external to a home/office.
iii. Monitored gardens and gates of neighbours.
iv. Monitored roads, neighbours, personal interactions through Dash Cams.

People do have rights to monitor protected spaces through CCTV systems. Protected space data also does have a value to third parties such as the police or city planners or even persons passing by an installed camera. A GDPR solution is certainly required for these spaces.

4) USE-CASES

The following are some use-cases to help establish the form of GDPR compliance required. These use-cases are based upon those given by the Information Commissioners' Office of the U.K. [20].

UC1: Police Monitoring - If the suspected movements of drug dealers are being monitored and recorded by the police with covert surveillance equipment in order to identify if they are committing any related offences then the level of privacy impact can be higher (No mandatory GDPR compliance is necessary). However, notice that overall the police are expected to be GDPR-compliant. For example, the police are not allowed to install covert cameras in subjects' homes or in private places like bathrooms.

UC2: Parking - If cars parked in a car park or on roads (in front of homes) get frequently damaged and broken into at night, or whether improved lighting affects the performance of CCTV for spotting the criminals or not. (Protected + Public Space – mandatory GDPR compliance is necessary.)

UC3: Neighbourhood - If the CCTV monitors the inside of a hospital, or monitors a High street shopping area, then it is subject to different privacy expectations. (Private + Protected Space – mandatory GDPR compliance is needed.)

UC4: Physical Scanning - Footages obtained from cameras covering the entrance to a drug rehabilitation centre will require captured images of people moving in and out to be obscured, as these images are considered sensitive personal data. Otherwise, this type of monitoring will lead to an unfair intrusion into the privacy of the individuals. Conversely, footage of an individual's movements in a bookshop is far less likely to require obscuring, due to the non-sensitive nature of the location. (Protected Space – mandatory GDPR compliance is required.)

IV. DATA PROTECTION-BY-DESIGN THROUGH TECHNOLOGY

Article 25 focusses on Data Protection-by-Design and -by-default (refer also to Section II.A). Data Protection-by-Default ensures data minimisation in the recording. That is to say only necessary information related to a data subject is collected and retained in the recording. If Data Protection-by-Design is implemented with proper technical measures, it will automatically ensure Data Protection-by-Default.

Data Protection-by-Design is an essential technical concept that should be considered during an implementation of a surveillance system. It means "safeguards provided to the personal data through technological design". Currently, for the management of Big Data, manual systems are replaced by automatic systems. The processing and handling of data procedures are best adhered [21] to when they are integrated in the technology. Nevertheless, there is still uncertainty about how Data Protection-by-Design is implemented in GDPR-complaint solutions. The regulations leave protective measures for visual privacy completely open. In the literature, numerous automated video redaction methods are proposed and implemented for effective visual protection. This current paper has classified and discussed them as reversible (Pseudonymisation) and irreversible (Anonymisation) visual protection techniques (Section II). The paper now highlights video redaction methods by incorporating the roles of computer vision, image processing and cryptography in the succeeding sections.

A. VIDEO REDACTION FOR VISUAL DATA PROTECTION

Video redaction is a method of obfuscating the personally identifiable and sensitive information of a data subject within any video. It is applied through different automated methods to ensure privacy is preserved at the time of capturing or storing videos. In redacted videos, whole object (individual), faces, background, and complete video frames can be deformed automatically so as to make the data subject unidentifiable and unrecognizable. In redaction-based software [22], two components are important: (1) Object Detection/tracking; and (2) Object obfuscation methods. Video redaction can be applied manually by detecting objects or Regions-of-Interest (ROI) or automatically by tracking an object.

1) ROLE OF COMPUTER VISION

Computer Vision (CV) is a sub-domain of Artificial Intelligence (AI). Any expert/intelligent system which processes visual information to recognize specific objects or ROIs within images [23] usually works through state-of-art computer vision algorithms. Such computer vision algorithms are increasingly robust when performing object detection and tracking.

Object Detection is the procedure of finding real-world instances, i.e. objects such as faces, bodies, bicycles, buildings, and licence plates, in images or videos. Object-detection algorithms classically employ extracted features and learning algorithms to recognize instances of an object category. They then take advantage of object classification and localization techniques to achieve accuracy in their results. Thus, to make a secure Data protection-by-design solution for any CCTV system, CV works by ROI selection (manually) or by detection/tracking (automatically) through pattern recognition and learning techniques (including Deep learning). Afterwards visual privacy protection methods will be applied through video redaction.

Currently, there are frequently utilized, pre-trained models for object detection including: YOLO (You Only Look Once) [24], Regional CNN (RCNN), Fast RCNN, Mask RCNN [25], and Multibox [26].

Object Recognition is based on: template matching; color matching; shape-based matching; or facial landmark detection (by locating the facial key points (15 to 68 unique points)). In the case of faces, these key points mark important areas of the face, such as the eyes, corners of the mouth, and the nose.

2) ROLE OF IMAGE/VIDEO PROCESSING

Image/video processing is extensively used to provide visual protection to CCTV surveillance videos. Image processing is the manipulation of a digitized image to improve (or deteriorate) the visual quality of given image. It comprises of different types of manipulations. For example: (1) image segmentation is employed to identify the pixel color-based information from images; (2) geometric transformations (enlargement, reduction, and rotation) may take place; (3) there may be a combination or blending of images; (4) image editing may take place; and (5) there could be interpolation [27].

For quick safeguard methods, GDPR emphasizes the word ''Pseudonymisation'' fifteen (15) times in the regulation, separate to the term Encryption. The term 'anonymous data' occurs once in Recital 26 [28]; otherwise, the term anonymisation is not discussed within the whole regulation. For the convenience of applying pseudonymisation as a GDPR-compliant solution, companies provide masking to detected objects in the visual data. Thus, most CCTV controllers consider masking as the pseudonymised solution, which is wrong in the light of the definition given in Section II.C.

It is worth mentioning here that irreversible schemes can only technically revert back to an original or can be identified/recognized again, if the originals are saved in storage for re-access. Most AI-based tools accessed over the Internet save originals for recovery of the manipulated image. Widely-used video redaction methods are classified in Table 2 and summarized after the Table. Fig. 5 shows the visual effects (produced by in-house experiments) of these methods applied to an image.

TABLE 2. Irreversible vs. reversible video redaction techniques.

Irreversible Video Redaction Techniques (Anonymisation)		Reversible Video Redaction Techniques (Pseudonymisation)	
(a)	Blurring	(a)	Scrambling with a key
(b)	Pixelation	(b)	Tokenization
(c)	Mosaic	(c)	False Colors
(d)	Cartooning	(d)	Encryption (in any form) (see Section IV.A .3)
(e)	Masking		
(f)	Warping		
(g)	Morphing		
(h)	Visual Abstraction (Face and body replacement/removal)		

(*a*) ***Blurring:*** This redaction method [29] is applied through image filters. The blurring filters can be applied to a complete video frame or some specific region/object, such as a face, person, licence plates, or signage. Common blurring filters are: (1) Mean filter; (2) Weighted average filter; and (3) Gaussian filter. For effective blurring, the Gaussian filter is utilized in most privacy-protection applications.

(*b*) ***Pixelation:*** The process of enlarging pixels within images to give them a blurred effect is known as pixelation [30]. It is also performed through pixel interpolation for high distortion effects. Interpolation works in two directions by using known data points to estimate the values at unknown points. Thus, image interpolation occurs in the distortion of an image from one-pixel grid to another grid.

(*c*) ***Mosaic:*** Small blocks of pixels from different regions are combined to give an un-identifiable effect to the picture [31], e.g. a face is obscured through pixel blocks taken from different areas of an image

(*d*) ***Cartooning:*** This is an image distortion technique which uses blurring filters and pixelation together 32] to give robust privacy to videos.

(*e*) ***Masking:*** The process of hiding visual information by replacing the original data with some unknown data.

(*f*) ***Warping:*** The process of distorting shapes in images by digitally manipulating them to hide the original shape. The warp is applied [33] by first transforming the location of pixels with a vector and then linearly interpolating the image.

(*g*) ***Morphing:*** This is a fluid transformation from one image to another. Images are morphed [33] by cross dissolving cuts in images.
Morphing is equivalent to warping (shape) plus cross-dissolving (colors)
Morphing, warping, face swapping are done through Facial Landmark detection.

FIGURE 5. **Privacy-protected video redaction techniques in image processing.**

(*h*) ***Visual Abstraction:*** The process of visual abstraction [34] is the replacement of objects/persons appearing in images by a visual model to protect the privacy of the individual, while enabling that person's activity. Abstraction can be obtained in a variety of ways: Change the face of a person to some cartoon face; apply a 3D avatar (Fig. 5) to the person's whole body; use a silhouette or blind box; and so on. Complete removal of the object within an image is also considered to be visual abstraction. This abstraction can be reversible if applied through tokenization (discussed below).

(*i*) ***Scrambling:*** Scrambling [35] refers to the permutation of data within an image. The formal definition of permutation is the re-ordering of data through specific patterns or at random. If scrambling is done through defined patterns or with a seed value, then this is called a reversible technique and data can be retrieved by using pattern information and a seed value. On the other hand, if scrambling is by a random re-ordering then it is known as an irreversible technique.

(*j*) ***Tokenization:*** Tokenization [36] is basically a non-mathematical data security method and a reversible technique. The process of tokenization is the swapping-out of sensitive information and the replacement of it with random numbers. The original and mapped numbers are separately stored in tables. This also works well in those code systems that rely upon codebooks and which act to transform plaintext into code-text. It is also widely used for securing credit/debit card numbers. In visual data tokenization, swapping of image pixels randomly with other values, is known as scrambling [35]. While, for complete object replacement, this can be implemented as a visual abstraction [34] as discussed above.

(*k*) ***False Colors:*** In this method [37], **i**mage privacy protection is achieved through mapping the original image to some other colour palette. It is a reversible technique and the original colours are reversed back to the original.

(*l*) ***Hashing:*** This is an irreversible technique [38] for converting arbitrary sized data to fixed size data. It is used for image indexing or finding the same images in a database. However, it cannot obfuscate images. Many GDPR blogs discuss this as a data security process but, in fact, it cannot be used for the redaction of visual data [39].

3) ROLE OF CRYPTOGRAPHY

Cryptography is the practice and study of data securing techniques [40]. Cryptography is a reversible process using encryption and decryption methods. In fact, encryption is the only reversible solution (through decryption) designated by the GDPR in its Articles. In the context of CCTV video, encryption can act on all or part of the video material with the intent of protecting the privacy of individuals captured by cameras and appearing within the video footage.

Thus, encryption is the process to make the original data (plaintext) into an unintelligible form (ciphertext) by means of encryption algorithms known as ciphers, with some specific random secret value(s) known as a key. For visual data protection, encryption is applied with the cipher and symmetric or asymmetric key/s over the full or part of a CCTV video. The cipher with the same or different key serves to decrypt the ciphertext in symmetric or asymmetric cryptography respectively. The regions or some important information such as color pixels or motion in videos can be identified by image processing and computer vision methods and then encryption acts as a safeguard for reversible obfuscation of visual data. There are many forms of encryption [41] which can provide some measure of protection. For example, there are:

1) ***Naïve Encryption:*** Full video encryption with a suitable block cipher. The encrypted video is not playable through video recorders and cannot be watched without decryption.
2) ***Selective/Sufficient Encryption:*** Specific parts/objects in the videos are detected and then encrypted. In the literature, other words i.e. ROI-based, soft, lightweight and partial encryption are also applied to this type of encryption. The videos are obfuscated in a way that they are viewable but not recognizable. The obfuscated videos may remain format compliant, and playable in the distorted form. The obfuscation is applied by strong ciphers, so that the adversary is not able to reconstruct the recognizable version through inference attacks [42].
3) ***Transparent/perceptual encryption:*** This is applied over multiple versions of a video [43]; a lower quality version is free to view but to view a full-quality version, the encryption key is required. Consequently, this method of encryption is applicable to the pay-per-view industry.

In cryptography, the robustness of the applied encryption is estimated through the robustness of the cipher and the length of secret key/s to avoid perceptual attacks on videos and brute force attacks on the keys. Numerous state-of-art algorithms have been proposed and tested in the last three decades to provide confidentiality to the data. The prevailing ciphers are DES, AES, RC4, and RSA, though DES has been largely replaced by AES because it can easily be broken by a brute-force attack (trying with all possible keys) with current PCs and RC4 has recently been broken by cryptographers [44]. For a secure key, a key space greater than 2^{100} is resilient to brute force attacks up to 2020 (by virtue of the time needed to guess every key possibility) [45]. Selective encryption on the carefully chosen video syntax elements within a large volume of videos data has proven to be strong, and, hence, cannot be easily cryptanalyzed [46].

It is noted here that there is always a trade-off between security and computational complexity when applying cryptography to visual data. The block-algorithm generally-considered to be the strongest, the Advanced Encryption Standard (AES) [47], has a complex set of sixteen rounds to compute using a minimal 64-bit block size (longer key lengths are available), which takes almost four times as much time than when the video is encrypted with a lightweight cipher (see Fig. 11, [48]). Selective encryption is the most adoptable way to obfuscate visual data because it takes much less encryption time to secure the video than the naïve or full form of encryption.

B. MARKET-BASED DATA PROTECTION-BY-DESIGN SOLUTIONS

This section surveys current Data protection-by-design solutions, operating globally within the commercial market place. Some provide reversible solution with encryption while the majority solutions only use video redaction through irreversible techniques.

StratoKey, [49] is a data protection-by-design solution for cloud and Software-as-a-Service (SaaS) for EU clients. This solution incorporates authentication and access controls for accessing personal data over a third-party cloud. StratoKey divides data into layers. This layering adds to the existing security, while providing a stringent form of additional security. StratoKey also provides Rule-based Security and Policy enforcement tools such as real-time Data Loss Prevention, geographical access fencing, device profiling and other measures to ensure security and data privacy. Specifically, StratoKey supports 'best-in-class' Federal Information Processing Standard (FIPS) 140-2 validated AES encryption using a 256-bit key and Format-Preserving Encryption algorithms. In addition, StratoKey has in-built support for standard key rotations. StratoKey also supports locking encryption keys to individual applications and even individual groups of users. These encryption key management features are native features within the StratoKey product. StratoKey also supports third- party key management services via the Key Management Interoperability Protocol (KMIP). In fact, it provides both hardware and software security.

Smartcrypt, [50] provides an on-the-spot encryption solution with Transparent Data Encryption (TDE) to the sensitive data of EU citizens. Smartcrypt encrypts sensitive data at its creation time and saves it in the encrypted form. This Smartcrypt encryption stays with the data even when it is moved and replicated to other user devices, file servers, or external systems. Smartcrypt employs the AES cipher in Cipher-Block-Chaining (CBC) mode with a 256-bit key. For signing digital certificates, RSA 2048 Probabilistic Signature Scheme (PSS) with preliminary SHA 512 hashing of data is used. They (AES and RSA) have their own key storage and retrieval mechanisms and are implemented on existing Intel and IBM hardware accelerators.

Sighthound, [51] offers GDPR-compliant video redaction software to EU clients for public surveillance. This software is available as a plug-in for cloud services, or as a stand-alone product for Windows- and Linux-based servers. The software is implemented through CV and Deep Learning models for automatic detection of people, faces and licence plates in real-time. It can be applied through manual selection to blur specific objects such as street signs or animals. The software is also able to detect people's age and gender, as well as their emotions. An irreversible blurring technique is applied to the data subject.

An *Intelligent Video Analytics services* [52] for public safety organizations provides advanced features of redaction and facial recognition to help investigations by security agencies. This is a complete security model to monitor suspicious activities through cameras. In this software, an ROI is extracted and blurring is applied to specific ROIs.

The GDPR-compliant *securityRuntime (secRT)* [53] is implemented with the AES cryptographic algorithm along with appropriate key management for the protection of textual data. This includes the process of tokenization of sensitive data, e.g. on the digits of a credit card number. secRT applies encryption to the original digits before tokenization and it then stores them in a database only intended for tokens.

Genetec software provides encryption and authentication for videos by means of the Omnicast Internet Protocol (IP) video management system [54]. Genetec offers cloud hosting, storage and sharing of video, while Identity Cloak is a local application of the software (see next).

Facit Data Systems Identity Cloak, (https://ipvm.com/reports/cloak-identity) provides GDPR-compliant solutions for CCTV videos. It provides two modes of blurring, (a) standard, and (b) full body. In standard blurring, faces along with the upper body and arms are considered for blurring, while full-body blurring covers the entire body of a data subject. Identity Cloak's face detection performs more consistently than Genetec Clearance, at higher angles of incidence, while also not losing faces as persons move away from the camera or across the field of view.

Pro Pixelated (https://www.propixelated.ie/) solutions use irreversible pixelation for static CCTV images. They provide the services of full face, complete image, number plate and other types of sensitive data blurring (pixelation) to EU clients.

Kinesense [55], offers video redaction services for CCTV videos. Irreversible masking and pixelation techniques are provided through annotation. An ROI is masked and pixelated through secure filters and areas outside the ROI can be pixelated for the purpose of location hiding.

Redaction, uses the concept of blurring and pixelation for ROI-based video redaction. The software provides GDPR-compliant solutions for body-worn cameras and drone footage and also provides CCTV anonymization (https://www.redaction.ie/).

Face404 software [56] performs the blurring of selected ROIs, e.g. human faces in a video. The Face404 (based on AI and CV) is a secure cloud-based solution, which meets the requirements of GDPR compliance for stored videos.

C. LIMITATIONS OF EXISTING SOLUTIONS

The majority of market-based solutions discussed above provide irreversible solutions, such as pixelation and blur, making that data no longer subject to GDPR. However, as discussed in Section II-C, this type of data storage is not useful for future purposes, even for legal use by supervisory authorities and stakeholders. Some surveyed market-based solutions provide encryption-based reversible and robust solutions by means of the AES cipher but mostly they are applied to textual data, not videos. Thus, there is a need for reversible and reliable visual Data protection-by-design solutions in the future.

Surveillance data collection companies should understand that the video redaction-based irreversible solutions are not sufficient in themselves. There is a pressing role for computer vision, image processing, and cryptography along with secure key management solutions [57] to provide a complete privacy protection model to visual surveillance data. Therefore, all these information technology domains must be combined together to provide a robust Data protection-by-design solution for the surveillance industry.

V. FORTHCOMING DATA PROTECTION-BY-DESIGN SOLUTIONS

Data protection-by-design solutions must ensure the four security services, i.e. confidentiality, integrity, availability and resiliency (Article 32(1)). For effective GDPR-compliant CCTV surveillance application, the following basic requirements must be considered by future researchers and developers:

1) Perceptual Security: The footage is effectively visually distorted and proof against attacks to remove that distortion. Here, the term "effectively" means that the distortion level within the video is sufficient to make video unwatchable. The video can be viewable but not understandable or pleasantly watchable.

2) Reversibility: The implemented safeguard should be reversible, so that the video can be used for legal purposes, if required.

3) Intelligibility: The activity level in the footage should not be obscured to prevent the identification of unethical/unlawful behaviors. However, notice that this requirement may be very difficult to be implement because: (i) there is no common definition of "unethical" behaviors; and (ii) unlawful behaviors vary between different EU states.

4) Efficiency: Camera devices operated with reduced hardware specifications (such as the Raspberry Pi and CMOS sensors) need real-time and efficient privacy-protection solutions.

5) Format compliance: Secured footage should be decodable within video players in an obscured/unintelligible form.

Thus, Data protection-by-design encompasses a complete technical solution, which may further include authentication, access rights, digital evidence chain, video records storage, and a method of generating successive secret keys from

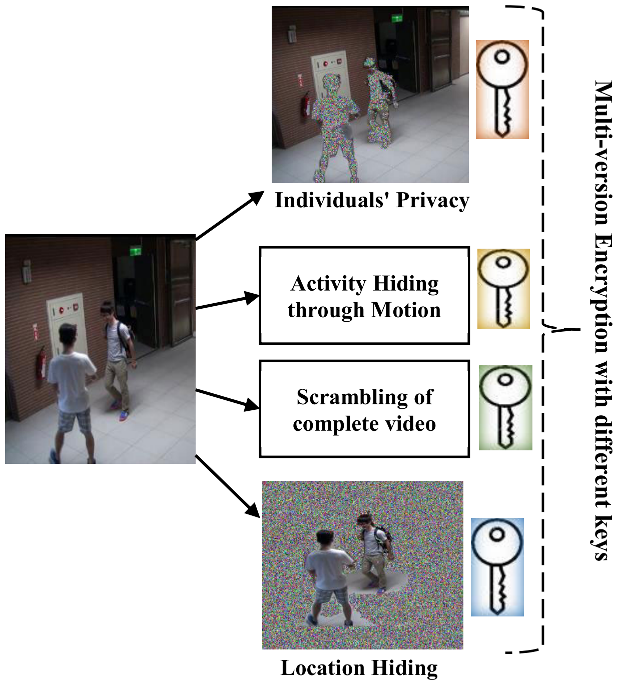

FIGURE 6. An example of a suggested multi-version encryption.

previous ones. The following are some suggestions for implementing Data protection-by-design solutions for visual data:

1) MULTI-VERSION ENCRYPTION

To provide privacy to visual data, multiple versions of the video footage can be created with different forms of reversible encryption. Naïve encryption is computationally expensive. Therefore, ROI-based and selective/lightweight encryption is desirable and it can be applied to the original video with different levels of confidentiality. The lightweight encryption stages can be utilized well for the purpose of anonymisation at the times of video capturing, streaming, and storage. For instance: (1) The foreground features of the footage can be encrypted for individual/object secrecy; (2) The background of footage can be obfuscated for location hiding; (3) Only motion in the footages can be encrypted to provided anonymity to activities in the footage; or (4) The pixel information of the whole video can be scrambled for complete confidentiality (see Fig. 6). These four usages can be encrypted through four different keys and the keys can be generated through state-of-the-art key management protocols and session keys may be managed by the blockchain technology discussed in part 3 of this Section.

2) ACCESS-CONTROLS FOR AUTHENTICATION

The above four scenarios can provide access controls to specific users. Law enforcement authorities, defence companies, and the police only accept original videos. They also have the right to access the whole video for investigation, while other stakeholders (third party/persons) do not need the original, whole videos. The specific key will be given to each user and they can only view the data according to their access rights.

Our proposed model will work almost in the same way as given by the authors in [58]. In [58], the authors' privacy console manages operator access to different versions of video derived data according to access-control lists, but without encryption.

3) BLOCKCHAIN

A Blockchain [59] is a system for ensuring the trust and integrity of transactions made on different machines. It works through hashing algorithms, which were first used for cryptocurrencies [60]. Notice that in some circumstances, such as when all participants are known to each other and several are known or thought to be trustworthy, then a Blockchain may be over-cumbersome. Classical signatures may then be more than sufficient to protect data integrity. However, Blockchains are a technologically innovative solution, which according to circumstances, may be a good solution.

A Blockchain has three main properties, i.e. Decentralization, Transparency, and Immutability, which are the factors that have contributed to the success of this technology in domains such as digital currencies. There are at least three possible forms of blockchain:

1) **Public blockchain:** The data is shared with no access restrictions on the participants and similarly any validator can voluntarily validate the shared data. This strategy is getting more attention due to inherent monetary benefits for validators. Digital currencies such as Bitcoin and Ethereum are well-known examples of public blockchain technologies.
2) **Private blockchain**: Contrary to the public blockchain, a private blockchain enforces a registration and an approval mechanism, both for participants and validators. This approach benefits the authentication and authorization of shared data for the known participants, maintaining a reliable chain of custody.
3) **Hybrid blockchain:** A combination of public and private blockchain systems in which multiple companies can exercise control. This hybrid approach by nature is permissioned and semi-decentralized.

The following analysis of the Digital Evidence Chain, includes two possible blockchain-based solutions for privacy protection of visual data, using either a private blockchain or a public blockchain. As is noted, the likely access pattern may well determine which (if any) of these options is chosen.

Digital Evidence Chain: Blockchain technology can be used for secure video evidence management in CCTV systems [61], as it is an effective solution for securing crime-scene evidence. In this solution, for each video footage transfer (transaction) from the controller to the supervisory authority, courts or other stakeholder, the cryptographic hash through SHA (256) [62] can be created at the start or after any modification by a third party within the chain. If any modification is made to that video by the data controller or

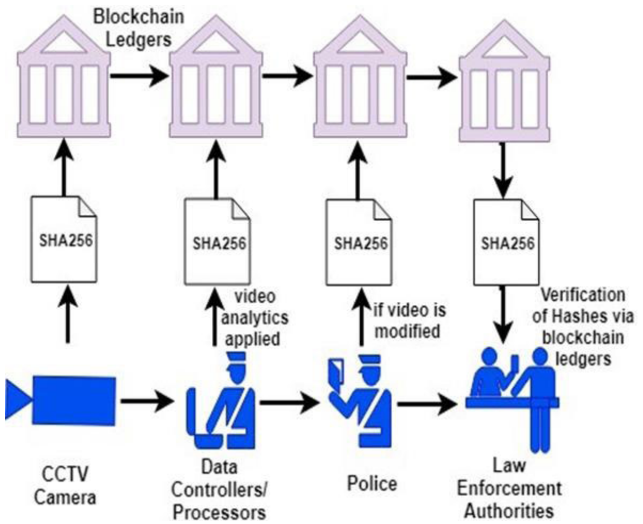

FIGURE 7. Suggested secure video evidence management chain.

the police, a new hash across the video footage, along with a time-stamped value, will be created. The hash must be stored in a separate table and also embedded within the transferred footage.

An example of a blockchain with three known participants i.e. controller, police and court is shown in Fig. 7, in which the generated hashes will make an integrated chain on each transfer, while maintaining trust for final verification by the law enforcement authorities.

As per CCTV company requirements the controllers can use private, public and hybrid blockchain networks for their digital history management purpose [63]. If the identities of all participants/stakeholders are known in advance (as in Fig. 7) then a private blockchain network (such as Hyperledger Fabric and R3 Corda) should be selected rather than a non-private blockchain [64].

However, it is sometimes the case that all stakeholders are not known in advance. For example, a passer-by, who has been recorded by the CCTV system in protected space, may also be interested in the footage for his/her own safety after some serious incident. Notice that the passer-by may also be an EU visitor.

Due to the use of a Decentralized Leger System (DLS), this technology is presently tamper-proof. While implementing a digital evidence chain through DLS, CCTV companies should consider the data subject's Right to Erasure (GDPR-Article 17). Therefore, to satisfy Article 17, existing immutable blockchain technology is not sufficient. There should be some allowance in the history management chain such as stipulating that only calculated hashes over transferred data become part of the chain rather than the complete data from the evidence chain. Thus, if the original data is not transferred with the chain then there will be no issues for controllers or processors in terms of Article 17. GDPR Article 17 compliance within a blockchain is an open challenge for all researchers, which merits a future in-depth analysis.

In any case, when implementing any such DLS, Brewer's well-known Consistency, Availability, and Partition tolerance (CAP) theorem should be borne in mind because such a blockchain-based DLS is distributed. The CAP theorem states that only two of the three desirable CAPs can be maintained. For example, if consistency within the evidence chain is a priority, i.e. individual transaction consistency is a priority rather than eventual consistency, then it may not be possible to maintain high availability in terms of transactions per second when updating the digital evidence chain. Equally, it may not be possible to maintain network partition tolerance, i.e. allow the distributed system to recover from a network outage.

Keys Generation Evidence Chain: Likewise, blockchain technology can be utilized for the creation and management of cryptographic keys for data controllers, the police and the supervisory authorities. The private secret keys for the algorithm to decrypt the encrypted video for an authenticated receiver are generated with a secure hash value. The hash can be embedded within the key to track the originality of key generation and be transferred to other stakeholders. On every key transfer, the secure hash can be re-generated to verify the originality of a key. Otherwise, a compromised key will be discarded. Blockchain ledgers can operate along with standard key management algorithms [57] to strengthen the key-generation history management and the original key verification process.

VI. CONCLUSIONS

Video surveillance is a pervasive phenomenon throughout the world. Along with the self-evident benefits of surveillance applications, protecting an individual's privacy is a critical task that controllers must perform. An individual, who is being monitored through CCTV systems, has a fundamental right to protect their identity. To ensure the freedom rights of individuals, GDPR has come into force within the EU. GDPR is a regulation, rather than a directive, because it is directly and equally applicable in all EU member states.

The purpose of this current paper was to shed light on GDPR-compliant strategies aimed at visual privacy protection in the presence of CCTV surveillance. This paper covers GDPR Article 6 in relation to both methods for pseudonymisation and encryption; Article 25 for Data protection-by-design and also by default; Article 32 for secure data processing; and Article 35 for DPIS as a foundation for proposing visual protection solutions through technology. The paper gives insights into: The visual personal data of an individual; the premises or circumstances for GDPR-compliant surveillance; and the existing vs. future technological solutions for assisting GDPR policies.

GDPR places a strong emphasis on encryption due to its reversible nature and its robustness in resisting intrusion. However, cryptographic solutions are expensive in terms of implementation, software, hardware, and manpower. Companies need to hire appropriately-trained IT staff to handle and maintain the complex ciphers within their organizations, particularly when they export data to a third party. The third party may need to hire trained cryptographers to manage and edit that information.

Data protection-by-design is still at an immature stage and requires reliable secure technologies for the privacy provision of digitized visual data in the context of the regulation. Article 25 serves as a backbone for secure technology-based solutions and Article 32 clarifies the security services provided by those solutions. For instance, *Confidentiality* requires that personal data whether in storage or transit can only be accessed by authenticated persons/systems to avoid interception attacks. *Integrity* requires that any modification to personal data whether in storage or transit can only be performed by authenticated persons/systems with the consent of the data subject. *Availability* requires that certain hardware and software services can only be accessed by authorized persons/systems, a failing in which can be due to an interruption attack by which a system is spoiled or made unusable. *Resilience* ensures the robustness of the technology, which should restore itself to its original form after attacks.

To conclude, as visual privacy is of great importance, thus, there is a vital need to deploy complete Data protection-by-design solutions for affected companies. The paper has discussed technological solutions provided by companies and it further suggests improvements. In the opinion of this paper's authors, cryptography with video redaction, acting together or in isolation are not sufficient. Multiple information technology domains will need to work hand-in-hand to implement effective Data protection-by-design solutions for video surveillance systems. Clearly, an additional cost will ensue in order to mitigate the privacy risks arising from the use of visual data. However, this cost will result in a meaningful implementation of GDPR-compliance by video surveillance companies, which will have a positive impact upon EU businesses. Importantly, similar solutions will become necessary outside the EU, if not already implemented and they are already necessary for those companies interacting with EU clients from outside the EU.

ACKNOWLEDGMENTS

We would like to thank the reviewers for their valuable comments in improving the quality of the article and in enhancing the readability and usefulness of our manuscript.

REFERENCES

[1] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU general data protection regulation: Changes and implications for personal data collecting companies," *Comput. Law Secur. Rev.*, vol. 34, no. 1, pp. 134–153, Feb. 2018.

[2] G. Pillai. (2012). *Caught on Camera: You are Filmed on CCTV 300 Times a Day in London*. Accessed: May 2019. [Online]. Available: https://www.ibtimes.co.uk/britain-cctv-camera-surveillance-watch-london-big-312382

[3] A. Cavallaro, "Privacy in video surveillance," *IEEE Signal Process. Mag.*, vol. 24, no. 2, pp. 166–168, Mar. 2007.

[4] Q. M. Rajpoot and C. D. Jensen, "Video surveillance: Privacy issues and legal compliance," in *Promoting Social Change and Democracy Through Information Technology*, V. Kumar and J. Svenson, Eds. Hershey, PA, USA: IGI Global, 2015, ch. 4, pp. 69–92.

[5] R. Furlong. (2006). *BBC NEWS | Europe | Germans Probe Merkel Spy Camera*. Accessed: May 2019. [Online]. Available: http://news.bbc.co.uk/2/hi/europe/4849806.stm

[6] Scottish Court. (2017). *£17,000 Damages Awarded by Scottish Court in Neighbour CCTV Dispute | Brett Wilson LLP*. Accessed: May 2019. [Online]. Available: https://www.brettwilson.co.uk/blog/17000-damages-awarded-scottish-courtwooley-wooley-v-nahid-akbar-akram-2017-sc-edin-7-neighbour-cctv-dispute/

[7] EU GDPR. (2016). *EUR-Lex–32016R0679–EN–EUR-Lex*. Accessed: May 2019. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[8] C. Babel. (2017). *Privacy and the EU GDPR US and UK Privacy Professionals*. [Online]. Available: http://www.corporatecomplianceinsights.com/wp-content/uploads/2017/11/TrustArc-Privacy-and-the-EU-GDPR-Research-Report-09.26.17.pdf

[9] G. Mainard. (2018). *Data Protection Issues*. Accessed: Jun. 2019. [Online]. Available: https://www.localenterprise.ie/DublinCity/Start-or-Grow-your-Business/Knowledge-Centre/eBusiness/Data-Protection-Issues/

[10] D. George, K. Reutimann, and A. Tamò-Larrieux, "GDPR bypass by design? Transient processing of data under the GDPR," *SSRN Electron. J.*, Aug. 2018.

[11] G. Petro. (2018). *Facebook's Scandal and GDPR are Creating New Opportunities for Retail*. Accessed: Jul. 2019. [Online]. Available: https://www.forbes.com/sites/gregpetro/2018/05/27/facebooks-scandal-and-gdpr-are-creating-new-opportunities-for-retail#481601a6626c

[12] Data Protection Commission. (2018). *Anonymisation and pseudonymisation | Data Protection Commissioner*. Accessed: Feb. 2019. [Online]. Available: https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation

[13] S. Stalla-Bourdillon and A. Knight, "Anonymous data v. personal data-false debate: An EU perspective on anonymization, pseudonymization and personal data," *Wisconsin Int. Law J.*, vol. 34, no. 2, pp. 284–322, 2017.

[14] S. Gilad-Gutnick, E. S. Harmatz, K. Tsourides, G. Yovel, and P. Sinha, "Recognizing facial slivers," *J. Cogn. Neurosci.*, vol. 30, no. 7, pp. 951–962, Jul. 2018.

[15] I. Bouchrika and M. S. Nixon, "People detection and recognition using gait for automated visual surveillance," in *Proc. IET Conf. Crime Secur.*, 2006, pp. 576–581.

[16] V. B. Semwal, N. Gaud, and G. C. Nandi, "Human gait state prediction using cellular automata and classification using ELM," in *Proc. Mach. Intell. Signal Anal.*, 2019, pp. 135–145.

[17] *Handbook No. 1: The Right to Respect for Private and Family Life. A Guide to the Implementation of Article 8 of the European Convention on Human Rights*, European Court of Human Rights, Strasbourg, France, Dec. 2001.

[18] L. van Zoonen, "Privacy concerns in smart cities," *Government Inf. Quart.*, vol. 33, no. 3, pp. 472–480, 2016.

[19] R. Buyya, S. T. Selvi, and X. Chu, *Object Oriented Programming With Java: Essentials and Applications*. New York, NY, USA: McGraw-Hill, 2009.

[20] Information Commissioners' Office (ICO). *In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information Version 1.2.*. Accessed: Jul. 2019. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection-1998/encryption/scenarios/cctv/

[21] A. Romanou, "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise," *Comput. Law Secur. Rev.*, vol. 34, no. 1, pp. 99–110, 2018.

[22] S. Sah, A. Shringi, R. Ptucha, A. M. Burry, and R. P. Loce, "Video redaction: A survey and comparison of enabling technologies," *J. Electron. Imag.*, vol. 26, no. 5, 2017, Art. no. 051406.

[23] P. Sinha, B. Balas, Y. Ostrovsky, and R. Russell, "Face recognition by humans: Nineteen results all computer vision researchers should know about," *Proc. IEEE*, vol. 94, no. 11, pp. 1948–1962, Nov. 2006.

[24] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2016, pp. 779–788.

[25] K. He, G. Gkioxari, P. Dollár, and R. Girshick, "Object detection for dummies part 3: R-CNN family," Facebook AI Res., New York, NY, USA, Tech. Rep., 2017.

[26] Z. Li and F. Zhou, "FSSD: Feature fusion single shot multibox detector," Dec. 2017, *arXiv:1712.00960*. [Online]. Available: https://arxiv.org/abs/1712.00960

[27] J. R. Padilla-López, A. A. Chaaraoui, and F. Flórez-Revuelta, "Visual privacy protection methods: A survey," *Expert Syst. Appl.*, vol. 42, no. 9, pp. 4177–4195, 2015.

[28] M. Mourby, E. Mackey, M. Elliot, H. Gowans, S. E. Wallace, J. Bell, H. Smith, S. Aidinlis, and J. Kaye, "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK," *Comput. Law Secur. Rev.*, vol. 34, no. 2, pp. 222–233, 2018.

[29] J. Flusser, S. Farokhi, C. Höschl, T. Suk, B. Zitová, and M. Pedone, "Recognition of images degraded by Gaussian blur," *IEEE Trans. Image Process.*, vol. 25, no. 2, pp. 790–806, Feb. 2016.

[30] T. Gerstner, D. DeCarlo, M. Alexa, A. Finkelstein, Y. Gingold, and A. Nealen, "Pixelated image abstraction with integrated user constraints," *Comput. Graph.*, vol. 37, no. 5, pp. 333–347, 2013.

[31] Y. Kusama, H. Kang, and K. Iwamura, "Mosaic-based privacy-protection with reversible watermarking," in *Proc. 12th Int. Joint Conf. e-Bus. Telecommun.*, Jul. 2015, pp. 98–103.

[32] A. Erdélyi, T. Barát, P. Valet, T. Winkler, and B. Rinner, "Adaptive cartooning for privacy protection in camera networks," in *Proc. 11th IEEE Int. Conf. Adv. Video Signal Based Surveill.*, Aug. 2014, pp. 44–49.

[33] J. Gomes and L. Velho, "Warping and Morphing," in *Proc. Image Process. Comput. Graph.*, 1997, pp. 271–296.

[34] K. Chinomi, N. Nitta, Y. Ito, and N. Babaguchi, "PriSurv: Privacy protected video surveillance system using adaptive visual abstraction," in *Advances in Multimedia Modeling—MMM* (Lecture Notes in Computer Science), vol. 4903, S. Satoh, F. Nack, and M. Etoh, Eds. Berlin, Germany: Springer, 2008, pp. 144–154.

[35] F. Dufaux, "Video scrambling for privacy protection in video surveillance: Recent results and validation framework," *Proc. SPIE* vol. 8063, May 2011, Art. no. 806302.

[36] T. Spies and R. T. Minner, "System for protecting sensitive data with distributed tokenization," U.S. Patents 0 046 853 A1, Feb. 13, 2014.

[37] S. Çiftçi, A. O. Akyüz, and T. Ebrahimi, "A reliable and reversible image privacy protection based on false colors," *IEEE Trans. Multimedia*, vol. 20, no. 1, pp. 68–81, Jan. 2018.

[38] V. E. Liong, J. Lu, Y.-P. Tan, and J. Zhou, "Deep video hashing," *IEEE Trans. Multimedia*, vol. 19, no. 6, pp. 1209–1219, Jun. 2017.

[39] A. Ewerlöf, "GDPR pseudonymization techniques," Medium Corp. (US), San Francisco, CA, USA, Tech. Rep., May 2018.

[40] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. London, U.K.: Chapman & Hall, 2005.

[41] H. Hofbauer and A. Uhl, "Identifying deficits of visual security metrics for images," *Signal Process., Image Commun.*, vol. 46, pp. 60–75, Aug. 2016.

[42] M. N. Asghar, M. Ghanbari, M. Fleury, and M. J. Reed, "Sufficient encryption based on entropy coding syntax elements of H.264/SVC," *Multimedia Tools Appl.*, vol. 74, no. 23, pp. 10215–10241, 2015.

[43] M. N. Asghar, R. Kousar, H. Majid, and M. Fleury, "Transparent encryption with scalable video communication: Lower-latency, CABAC-based schemes," *J. Vis. Commun. Image Represent.*, vol. 45, pp. 122–136, May 2017.

[44] A. Popov, *Prohibiting RC4 Cipher Suites*, Standard RFC 7465, IETF, Fremont, CA, USA, Feb. 2015.

[45] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[46] M. N. Asghar, M. Ghanbari, M. Fleury, and M. J. Reed, "Confidentiality of a selectively encrypted H.264 coded video bit-stream," *J. Vis. Commun. Image Represent.*, vol. 25, no. 2, pp. 487–498, 2014.

[47] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Berlin, Germany: Springer, 2002.

[48] A. Shifa, M. N. Asghar, S. Noor, N. Gohar, and M. Fleury, "Lightweight cipher for H.264 videos in the Internet of multimedia things with encryption space ratio diagnostics," *Sensors*, vol. 19, no. 5, p. 1228, 2019.

[49] StratoKey. (2018). *Technical White Paper*. Accessed: Feb. 18, 2019. [Online]. Available: https://www.stratokey.com/resources/stratokey-white-paper

[50] Pkware. (2019). *Smartcrypt Transparent Data Encryption (TDE) Reliable Encryption for Structured and Unstructured Data [Internet]*. Accessed: May 15, 2019. [Online]. Available: https://www.pkware.com/smartcrypt-tde

[51] Sighthound. *Computer Vision Software With Deeply-Learned AI Vision API & SDK's | Technology*. Accessed: Feb. 1, 2019. [Online]. Available: https://www.sighthound.com/technology/

[52] IBM. *IBM Intelligent Video Analytics—Overview—Ireland*. Accessed: Jul. 7, 2019. [Online]. Available: https://www.ibm.com/analytics/ie/en/

[53] EPeri. (2019). *Open Source—EPeri [Internet]*. Accessed: May 15, 2019. [Online]. Available: https://eperi.com/open-source/

[54] Clearance. (2019). *Omnicast | Genetec [Internet]*. Accessed: May 15, 2019. [Online]. Available: https://www.genetec.com/solutions/all-products/omnicast

[55] Kinesense. *Video Redaction for GDPR*. Accessed: Feb. 1, 2019. [Online]. Available: https://www.kinesense-vca.com/2018/05/25/kinesense-tips-tricks-18-gdpr-addition/

[56] SeekLayer. *SeekLayer—Fast, Affordable, GDPR-Compliant Video Redaction*. Accessed: May 15, 2019. [Online]. Available: https://www.seeklayer.com#cctv_redaction_section

[57] S. Bellovin and R. Housley, *Guidelines for Cryptographic Key Management*, Standard RFC 4107, IETF, Fremont, CA, USA, Jun. 2005.

[58] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, A. Ekin, J. Connell, C. F. Shu, and M. Lu, "Enabling video privacy through computer vision," *IEEE Security Privacy*, vol. 3, no. 3, pp. 50–57, May 2005.

[59] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, Jan. 2017.

[60] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.cryptovest.com

[61] M. Liu, J. Shang, P. Liu, Y. Shi, and M. Wang, "VideoChain: Trusted video surveillance based on blockchain for campus," in *Cloud Computing and Security—ICCS* (Lecture Notes in Computer Science), vol. 11066, X. Sun, Z. Pan, and E. Bertino, Eds. Cham, Switzerland: Springer, 2018, pp. 48–58.

[62] H. Vranken, "Sustainability of bitcoin and blockchains," *Current Opinion Environ. Sustainability*, vol. 28, pp. 1–9, Oct. 2017.

[63] H. Al-Khateeb, G. Epiphaniou, and H. Daly, "Blockchain for modern digital Forensics: The chain-of-custody as a distributed ledger," in *Blockchain and Clinical Trial* (Advanced Sciences and Technologies for Security Applications), H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, and H. Al-Khateeb, Eds. Springer-Verlag, 2019.

[64] K. Wüst and A. Gervais, "Do you need a Blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol.*, Jun. 2018, pp. 45–54.

MAMOONA N. ASGHAR received the Ph.D. degree with the School of Computer Science and Electronic Engineering, University of Essex, Colchester, U.K., in 2013. She has been a Marie Sklodowska-Curie (MSC) Career-Fit Research Fellow with the Software Research Institute, Athlone Institute of Technology (AIT), Ireland, since June 2018. As an MSC Principal Investigator (PI), her research targets the proposals and implementation of technological solutions for General Data Protection Regulation (GDPR) compliant Surveillance systems. She is also a regular Faculty Member with the Department of Computer Science and Information Technology (DCS & IT), The Islamia University of Bahawalpur, Punjab, Pakistan, where she is currently on postdoc leave. She has more than 14 years of teaching and R&D experience. She has published several ISI indexed journal articles along with numerous International conference papers. She is also actively involved in reviewing for renowned journals and conferences. Her research interests include security aspects of multimedia (image, audio and video), compression, visual privacy, encryption, steganography, secure transmission in future networks, video quality metrics, and key management schemes.

NADIA KANWAL received the M.Sc. and Ph.D. degrees in computer science from the University of Essex, Essex, U.K., in 2009 and 2013, respectively. She is currently a Marie Sklodowska-Curie Career-Fit Postdoctoral Fellow with the Software Research Institute, Athlone Institute of Technology (AIT), Ireland. The primary objective of this fellowship is to propose technological solutions for privacy protection of humans as per GDPR guidelines. She is also associated with the Lahore College for Women University, Pakistan, where she is also an Associate Professor and is also on leave to pursue Postdoctoral Fellowship. She is applying deep learning methods to improve the performance of vision algorithms for detection and matching tasks which can help to develop robust solutions for different vision-related applications. Her research interests include machine learning, image/video processing, medical imaging, and privacy. She remained a student member of the IEEE Computer Society, the Institution of Engineering and Technology, and the British Machine Vision Association. She has been actively involved in reviewing for reputed conferences and journals.

BRIAN LEE received the Ph.D. degree from the Trinity College Dublin, Dublin, Ireland, in the application of programmable networking for network management. He has over 25 years R&D experience in telecommunications network monitoring, their systems and software design and development for large telecommunications products with very high impact research publications. He was the Director of research for LM Ericsson, Ireland, with responsibility for overseeing all research activities, including external collaborations and relationship management. He was an Engineering Manager with Duolog Ltd., where he was responsible for strategic and operational management of all research and development activities. He is currently the Director of the Software Research Institute, Athlone Institute of Technology, Athlone, Ireland.

MARTIN FLEURY received the degree in modern history from Oxford University, U.K., the degree in maths/physics from the Open University, Milton Keynes, U.K., the M.Sc. degree in astrophysics from the QMW College, University of London, U.K., in 1990, the M.Sc. degree in parallel computing systems from the University of South-West England, Bristol, in 1991, and the Ph.D. degree in parallel image-processing systems from the University of Essex, Colchester, U.K. He was a Senior Lecturer with the University of Essex, after which he became a Visiting Fellow. He is currently associated with the School of Engineering, Arts, Science, Technology and Engineering (EAST), University of Suffolk, Ipswich, U.K. He is also a Free-Lance Consultant. He has authored or coauthored around 295 and book chapters on topics such as document and image compression algorithms, performance prediction of parallel systems, software engineering, reconfigurable hardware, and vision systems. He has published or edited books on high performance computing for image processing and peer-to-peer streaming. His current research interests include video communication over wireless networks.

MARCO HERBST received the degree in mechanical engineering from the Trinity College Dublin, in 1999. He has successfully leads several software development teams. As CEO and CTO of Jobs.ie and Evercam, he was responsible for leading a team of software developers to build Ireland's most popular recruitment website and CCTV systems. He worked on CCTV hardware, software and large-scale camera deployments for seven years. He is currently an Innovator in time-lapse and monitoring software for construction projects and urban CCTV systems, positioning his company Evercam Ltd., as a Market Leader in the sector.

YUANSONG QIAO received the B.Sc. and M.Sc. degrees in solid mechanics from Beihang University, Beijing, China, in 1996 and 1999, respectively, and the Ph.D. degree in computer applied technology from the Institute of Software, Chinese Academy of Sciences (ISCAS), Beijing, in 2008. He is currently a Senior Research Fellow with the Software Research Institute (SRI), Athlone Institute of Technology (AIT), Ireland. His research interests include the future Internet architecture, blockchain systems, the IoT systems, and edge intelligence and computing. He is a member of the IEEE (Communications and Computer Societies and Blockchain Community) and ACM (SIGCOMM and SIGMM).