CALL FOR INPUT

BY

AD HOC COMMITTEE TO ELABORATED A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES FOR CRIMINAL PURPOSES

TITLE:

USING TECHNOLOGY TO COMBAT CRIME AND PROMOTE THE RULE OF LAW

WRITTEN ARTICLE

BY

ASABE SHEHU YAR'ADUA FOUNDATION

Membership/Affiliates:

- UNITED NATION DEPARTMENT OF PUBLIC INFORMATION (UNDP/DPI)

- UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC)

- ECONOMIC AND SOCIAL COUNCIL (ECOSOC)

-Green Climate Fun (GCF)

- UNFCCC United Nations Framework Convention on Climate Change

- AFRICAN UNION

- EURPEAN UNION

- UNITED NATIONS COMMISSION ON HUMAN RIGHTS (OHCHR)

- UNITED NATION ENABLE, RIGHT OF PERSONS WITH DISABILITIES

- OFFICE TO MONITOR AND COMBAT TRAFFICKING IN PERSONS, U.S DEPARTMENT OF STATE

- GLOBAL MODERN SLAVERY

- GLOBAL FUND TO END SLAVERY

- WORLD ASSOCIATION OF NGOS (WANGO) AS A REGULAR MEMBER, USA

- WORLD CODE OF ETHICS AND CONDUCT FOR NGOS

- UNICEF USA IN THE FIGHT FOR CHILD SURVIVAL

- EUROPEAN COMMISSION WITH ID NO: NG-2009 FUI-3110223990

- NIGERIAN NETWORK OF NGOS (NNGO)

- NIGERIA – FEDERAL MINISTRY OF WOMEN AFFAIRS AND THE 36 STATES

- MINISTRIES OF WOMEN AFFAIRS

- NATIONAL COUNCIL OF CHILD RIGHTS ADVOCATES OF NIGERIA (NACCRAN)

- NIGERIA – NATIONAL AIDS CONTROL AGENCY AND STATE AGENCIES ON AIDS

- ROTARY CLUB INTERNATIONAL

- ECOSOCC AFRICA

- NATIONAL POPULATION COMMISSION

- NATIONAL HUMAN RIGHT COMMISSION

- INEC OBSERVER FOR GOOD GOVERNANCE

- UNESCO

- FEDERAL MINISTRY OF YOUTH DEVELOPMENT

- FEDERAL MINISTRY OF INFORMATION

- UNITED NATION MILLENNIUM DEVELOPMENT GOAL (MDGS)

- SUSTAINABLE DEVELOPMENT GOALS (SDGS)

Using Technology To Combat Crime And Promote The Rule Of Law

Criminal activity is a prevalent issue in contemporary culture and society, with most nations facing unacceptable levels of crime. Technological innovation has been one of the main driving forces leading to the continuous improvement of crime control and crime prevention strategies (e.g. GPS tracking and tagging, video surveillance, etc.). Given this, it is a moral obligation for the research community to consider how the contemporary technological developments (i.e. Internet of Things (IoT), Machine Learning, Edge Computing)might help reduce crime worldwide. After a thorough analysis of a wide array of technologies and a number of workshops with organizations of interest, we believe that the adoption of novel technologies by vulnerable individuals, victim support organizations and law enforcement can help reduce the occurrence of criminal activity.

"Technology enable criminals to work across regions; increasing their reach, their crimes and their profits. Just as the Internet has transformed every aspect of our lives, it has also become a cornerstone of criminality." In an increasing high-tech world, science, technology and innovation could be manipulated for criminal purposes.

Criminals manipulate new technologies to recruit and exploit victims of human trafficking or spread extremist ideologies. The internet can also serve as an illicit market for drugs, firearms or trafficked wildlife products and a 2018 study estimated that cybercrime cost approximatively 600 billion US dollars. In its resolution to counter the use of information and communications technologies for criminal purposes, the UN General Assembly shared its concern regarding "the increase in the rate and diversity of crimes committed in the digital world and their impact on the stability of critical infrastructure of States and enterprises and on the well-being of individuals."

Yet, to use the words of Maria Luiza Ribeiro Viotti, Chef de Cabinet for the UN Secretary-General, "the aspirations of the 2030 Agenda cannot be through business as usual" as technology and innovation have an important role to play reaching the Sustainable Development Goals. In this spirit, UNODC has been engaging with young people around the world especially coders to come up with technological ways to combat organized crime.

A. Technology-driven Solutions for Crime Prevention

The advent of pervasive computing and the IoT provides new potential opportunities for technology-driven solutions for crime prevention. We discusses the working principle of such technologies as well as (where appropriate) how these are currently used for preventing crime.

Camera-based Technologies:

In recent years, Closed Circuit Television (CCTV) surveillance has emerged globally as a mainstream crime prevention measure. CCTV technology is already present in many public places such as railway stations, airports, office buildings and on the street. Moreover, as early as 2005,

estimates suggest that in the United Kingdom there were already over 4 million cameras in place – an approximate ratio of 1 camera per 14 citizens. While CCTV cameras were formerly employed as a means to report crime, support police officers with prosecution processes or as a supporting evidence in court of justice, the increasing developments in computer vision and machine learning provide opportunities for investigating CCTV surveillance as a crime prevention mechanism. CCTV cameras are typically intended to reduce crime through several mechanisms. The first is to deter offenders who fear being identified committing a crime on camera. The second is to provide law enforcement agencies with an opportunity to identify crimes in progress or those that are about to happen, to provide them with an opportunity to intervene. Where these two mechanisms fail, CCTV cameras can record evidence that a crime occurred, who was involved and what took place, which can be used in criminal prosecutions. The first mechanism relies on offenders perceiving that CCTV is effective, otherwise there will be no perceived risk. The second relies on staff monitoring (possibly many) camera feeds and being able to identify suspicious activity. The third relies on the camera(s) being able to capture an event in progress, which may require it to pan and tilt accordingly. It is not hard to imagine why failures associated with human error might emerge, given the difficulties associated with these tasks. However, developments in computer vision and machine learning, which are leading to a continuous improvement in applications such as object and face recognition or gait analysis, clearly provide opportunities for CCTV surveillance that might enhance its effectiveness. CCTV surveillance systems are constantly being upgraded to incorporate the latest soft technology features. These include on-the-edge feature extraction and machine learning classification algorithms. As a result, it is now possible to extract different patterns and personal bio-metrics from video sequences, which can be a posteriori used for person identification. In this sense, CCTV technology has been investigated in different applications. These include the automatic detection of suspicious anomalies such us unattended bags in mass transit areas or crowded venues, iris recognition-based security systems which deny access to buildings to unauthorised personnel, intrusion detection systems (IDS) in unauthorised areas employing motion tracking techniques, automatic robbery detection in banks via object and human posture detection, and even as a means of crowd detection and congestion analysis for safety purposes.

Electronic Monitoring and Global Positioning System-based Technologies:

a. Electronic Monitoring (EM) began in the early 1980's in the US and spread rapidly after positive initial claims in reducing control deficits in community supervision. First EM systems employed radio frequency identification (RFID) technology. RFID technology is based on a tag with a unique identifier which sends data to an electronic reader through wireless radio frequency waves, enabling its identification and tracking. RFID technology was first employed to confine offenders (or pre-trial defendants) to a particular location (usually their home). The work in showed that placement of sex offenders on EM programs reduced the likelihood of and postponed their return to prison. The use of RFID technology was then extended to the protection of victims of domestic violence. Victims were provided with receivers so that they were alerted when an

offender was present within a pre-established control perimeter, which was normally set to be around the victim's home.

b. The second generation of EM technologies incorporated the use of Global Positioning System or GPS. GPS is a satellite-based global navigation system which provides geo-location through the use of a network of satellites orbiting the Earth at an altitude of approximately 20,200 km. To estimate the geo-location, a GPS receiver intercepts the signals of at least three network satellites at regular intervals of time. A posteriori, based on the time it takes to receive each of the satellite signals, the geo-location of the GPS receiver is calculated via trilateration. The use of GPS technology as a crime prevention tool has gained increasing attention since late 1990's. The ability to customise exclusion zones and provide instant alerts if these are violated, has extended the use of electronic monitoring to sex offenders and post-work release offenders.

Short-Range Wireless Communication Technologies

Short-range wireless communication transceivers such as Bluetooth and WIFI are widely incorporated into many portable and mobile devices, including laptops, mobile phones and smart-watches. During the manufacturing process, a wireless module is assigned a unique identification (ID) in the form of a 48-bit Medium Access Control (MAC) address. This address is then used to identify and authenticate a device when communicating with other wireless devices. For example, Bluetooth (BT) devices can interact with other nearby BT devices within their signal range (10m to 100m, depending on the radio transceiver) by sending and receiving radio waves within a band of 79 different frequencies centred at 2.45 GHz. Using such radio waves, along with the identification capabilities provided by the unique MAC address assigned, a Bluetooth device can continuously monitor other Bluetooth devices nearby (within its signal range) and also identify the type of device associated with such MAC address (i.e. whether it is a smart-phone or a laptop for example). In addition, the Received Signal Strength Indicator (RSSI) provides an estimated measure of the power present in a received radio signal. As shown by previous RF-based research, RSSI can then be used to estimate the approximate distance a Bluetooth receiver is from a Bluetooth emitter.

Exploiting the above characteristics of this technology, various researchers have employed Bluetooth technology to estimate the surrounding social context of a person or to estimate pedestrian flows at specific places.

Audio-based Technologies

Audio-based technologies have been used for many years to anticipate criminal actions. Common examples include the interception of calls by police officers (wire tapping) or the use of recording devices as evidence collection mechanisms. With the current advances in audio processing and machine learning techniques, whereby several parameters and bio-metrics can be automatically computed from raw audio recordings, the scope of audio-based technologies have experienced a great expansion. For instance, gun shot detection audio-based technologies have been recently evaluated in the US. Gun shot detection is a novel technology which employs a network of

microphones, typically installed in high crime areas, which discriminates gunshots from other types of noises and computes the spatial coordinates of the location where the shot was fired. Besides, the presence of Intelligent Virtual Assistants (IVAs) or Chatbots such as Amazon Alexa or Google Assistant is becoming increasingly popular . Such IVAs incorporate speech recognition capabilities allowing users for asking questions and making requests to different interfaces. In addition to speech recognition, it is now possible to count the number of speakers in a conversation via speaker diarization, to infer the sentiment (mood) of individuals by analysing their voice or yet recognise a speaker by his/her voice with considerably low error rates. These advances clearly provide opportunities for implementing audio-based crime prevention tools.

Affective Computing

Recent research has realised that there is a significant relationship between the physical health and emotional state of an individual. Given this, the field of affective computing is receiving increasing attention in the last few years. Affective computing or emotional intelligence is the study and development of systems for the 5 A PREPRINT - FEBRUARY 9, 2021 recognition, processing and interpretation of human affects. Typically, this is performed with the use of wearable devices or smart textiles by which various physiological signals related to stress levels are measured, processed and interpreted. Electro-dermal activity (EDA) and heart rate variability (HRV) are two major examples of physiological signals employed in affective computing. Although affective computing is still as its infancy, several studies have shown that such signals can be translated into relevant features which ultimately lead to estimations of human stress levels. For instance, the research studies in [50, 51] have made use of the MIT Stress Recognition in Automobile Drivers Database [52] to classify between three different stress levels (low, medium and high) in three different driving scenarios. Although, to the best of our knowledge, affective computing has not been employed in the context of crime prevention, the anticipation of high levels of stress could assist the prevention of crime. As suggested by literature in the field [53], mental disorder and violence may each be rooted in the stress levels at which an individual lives. On another note, mental disorder has been shown to increase the chances of committing crime. For instance, in the study conducted by [54] -using a Swedish birth cohort selected at random- it was found that men with major mental disorders were more than ten times more likely than men with no mental disorders to have criminal offense records and four times more likely to be registered for a violent offense. Other work [55, 56, 57] suggest that, on average, victims of domestic violence have poorer mental health, which can lead to further issues including depression or anxiety. Although as aforementioned, sentiment analysis is still at its infancy, this technology clearly shows the potential to be explored as a crime prevention mechanism.

Information-based Technologies

In addition to the technologies discussed above, a wide array of information-based crime prevention solutions have been developed in the last years. One of such technologies is Crime Mapping (CM), also known as hot-spot policing. CM refers to the process of conducting spatial analysis to map, visualise and analyse crime patterns. This allows for the identification of crime

hot spots in conjunction with other crime trends and patterns[60, 61]. Such information can then be used to optimise the location of human or/and technological resources. As various works suggest, the identification of hot spots is an effective software-based technology for optimising the use of resources and ultimately prevent crime [62, 63]. Risk assessment is another key information-based technology for crime prevention. Risk assessment is used to assess the risk of recommitting crime by offenders under correctional control. According to the survey conducted in [64], a majority of serious crimes are committed by a small fraction of people during the first months of probation parole. Risk assessment tools make use of predictive models to identify such subgroup of people so that appropriate surveillance/supervision is granted to those cases. Likewise, information technology is used to identify the likelihood of a terrorist attack or a serious violent event occurring at certain places, including schools, airports or train stations among others [12]. Another application where information technology has been adopted to prevent crime is in the development of computer software to track individuals' interactions on various social media sites [65]. The monitoring of such suspect's interactions is then used to identify abnormal behaviours which can potentially be related to crime intentions.

Crime Prevention Mobile Apps

The number of downloads of mobile apps has been steadily growing worldwide for the past decade. Along with this, the average time per day spent by adults on their smartphones is growing at a fast pace and this is forecasted to continue. For instance, in the UK, that figure is expected to go over 4 hours in 2026. With this in mind, the development of mobile apps as a means of crime prevention seems highly beneficial for promoting and enhancing social safety. In this context, a wide array of applications have been proposed to help either with the prevention of crime or with the reporting of crime that has already occurred. Apps for crime prevention can be broadly divided into two categories, namely apps to be adopted by policing institutions and those directed to the general public. The remainder of this section presents a wide array of mobile apps for crime prevention with a special focus on those related to the reporting of emergency situations.

Mobile Apps for Emergency Situations: Numerous mobile apps have been developed in recent years to facilitate the communication of emergency and panic situations to close relatives and policing institutions. For instance, Circle of 6 [67] is a mobile app that enables its users to quickly contact a user-defined list of six people and share their current location along with an emergency message. In a similar way, Noonlight [68] provides a mechanism to alert emergency institutions by pushing and holding a button embedded in the app. When the button is released, the user is asked for her/his pin number. A posteriori, the user just needs to enter the pin to indicate he or she is safe. If the pin is not provided, the situation is immediately reported to emergency institutions along with the live GPS geo-location of the user. A similar working principle to that of Circle of 6 and Noonlight is provided by Silent Beacon [69]. In this case, a portable device in the form of a panic button is provided alongside the app. Once the button is triggered, the device communicates the action to the smartphone app which then automatically calls 911 while

communicating the emergency situation and the location to a user-defined list of contacts. A similar functionality is offered by Red Panic Button [70], which in addition to the above features, incorporates the automatic publication of emergency messages on Twitter. Another example is bSafe [71], which allows a list of user-selected contacts to track the user's way home using GPS information. In addition, as with the apps presented above, it allows the communication of emergency situations while also collecting evidence in the form of audio and video recordings

Edge Computing and on Device Processing

Traditionally, the majority of the processing for data intensive applications was done on a central cloud to take advantage of fast and powerful computing infrastructure. However, major issues concerning latency, security and privacy can be identified in the use of cloud-based systems for crime prevention. In this regard, a new trend of processing the data on the edge is emerging. The motivation behind edge computing is that of performing the data processing as near as possible to the point of data production. With this, the privacy and latency issues present in cloud-based systems can be significantly mitigated. AI is gradually finding its way into embedding systems which are becoming smaller and less power demanding, while offering fast processing power and low latency at an increasingly attractive cost. A number of off-the-shelf edge computing devices suitable to carry out heavy signal processing and machine learning applications are already available (see Fig. 7). For instance, both Nvidia and Google have recently released their respective development boards, namely Jetson Nano and Google Edge TPU, with the aim of enabling users to develop and run AI applications on the edge. In addition to their portability and the privacy advantages they offer, such boards are supported by sophisticated development kits that consist of a SOM (System-on-Module) connected to a development board which incorporate numerous connectors like USB and Ethernet to share the data gathered when desired. Furthermore, the above devices also support major deep learning frameworks and tools such as TensorFlow. The above, alongside current developments in the field [76], suggest that edge computing is finding its way into city centers for the early detection and prevention of criminal actions.

Opportunities

CCTV surveillance has been widely employed to prevent and report crime under different circumstances. The continuous developments seen in pervasive computing as well as in computer vision, allow for the on-board computation of different bio-metrics (i.e. face recognition or gait analysis) and for the extraction of patterns which are key to identify suspects as well as activities taking place within its field of view. Despite the great potential shown by CCTV surveillance on preventing various type of crimes in public and outdoor places [13], several drawbacks are found on its application inside home environments (i.e. abusive relationships). First, after the installation, the device is typically visible. While this is paramount for applications where the aim is to deter crime, where the aim is to collect evidence surreptitiously it would be better to conceal the device. Second, a home CCTV surveillance system would require the installation of numerous CCTV cameras, since the view field is limited to the room at where the camera is

mounted. Third, CCTV cameras are sensitive to lighting conditions and occlusion (i.e. aggressive behaviour in the night could not be detected)

Feedback from End User Organisations and Practitioners

The opportunities new technologies present to monitor and prevent domestic abuse were explored during a series of workshops with academic experts, practitioners, and a selection of engineers and technologists, including representatives from police forces, government, charities, trusts, voluntary support groups and end users. Few workshops took place between June 2018 and May 2020. The content of the different workshops is summarised as follows: 1. Exploratory Workshops (World Cafes): We held two workshops to explore how developing technologies might help to reduce the risk of domestic abuse. The aim of the first workshop was to work with domain experts to produce a "requirements brief" that mapped out a handful of priority problems, together with any factors that constrain how they are dealt with now and how they might be dealt with in the future. The aim of the second workshop was to identify possible solutions to the problems identified. A mixture of domain experts, designers and engineers were invited to the second workshop.

Co-Design Workshop: Existing examples of crime prevention technologies were discussed to explore the opportunities they offer. Also, the difficulties that survivors might face in calling for help or recording evidence discreetly were discussed. Few potential technologies that might help in supporting both victims, police and aid evidence gathering were introduced. Participants particularly liked the portability of small Edge Computing platforms including wearable devices and the different methods of interaction as compared to smartphones. Participants were excited by the concept of proximity detection techniques being able to sense the presence of individuals and any abnormal activities in the surrounding environment and the nearby vicinity as many vulnerable individuals might find it difficult to record such incidents. The possibility for IoT devices to provide evidence and a reliable journal was also intriguing as the participants had not acknowledged these technologies before. 3. Co-Creation Workshop: A reduced number of possible technological solutions including tagging and proximity detection were discussed along with hand-on demonstrations. First the potential use of short range tagging technology as part of a panic alarm was discussed. The scenario proposed was one where small tags “dots” are placed in home environments, or in public places, which then can be used to send an alarm or as an information access point. Proximity detection technologies [84, 85] were also discussed due to their potential in ensuring regular offenders keep their legal distance from victims. Fig. 8 shows how the alerts can be sent out depending on the proximity of the devices of interest. An alternative suggestion considered the use of internet connected devices, such as smart speakers, to automatically detect incidents of abuse whilst these were in progress. To reduce false alarms, it was suggested that such a system could scan for multiple signals to include slammed doors, raised voices, particular keywords in verbal exchanges, or other indicators of threats of risk. We discussed the practicality of such a system and how to protect user’s privacy, as well as how triggering actions could be tailored to the individuals in question to increase the sensitivity of the

system. Once triggered, data can be stored locally or on the cloud, and alerts can be sent to trusted third parties. 4. One to one discussions with End Users Organisations: Based on the discussions in the previous workshops, the aim of these series of online discussions was to narrow down the possible development routes and to come up with a list of paper prototypes which were discussed with each organization to understand their implications and limitations. 5. Design Evaluation Workshop: In the last of these workshops, the previously discussed technologies narrowed down the proposed prototypes, including the use of short-range communication mediums for alert and recording of abnormal activities in close proximity and also the use of AI to detect violent behavior. During the workshop the discussion converged on the benefits of a single edge device aimed at crime prevention and the collection of evidence that would protect users privacy. The use of edge computing would mean that data would not need to be stored remotely and the available processing power would mean that computational intense processing (e.g. voice and sentiment detection) could be carried out on such a device. Personalized and more adaptable interfaces or functionalities of the device then can be developed targeting diverse groups of people.

Diversity and Scalability

Developing AI technologies to detect explicit personal behaviors' or actions requires the collection of data from a large number of users, to enable predictive models incorporate sufficient variability in order to generalize well on unseen data. Therefore, it is crucial to carry out data collection processes on a large number of experimental participants, as well as to consider the differences that may exist between different groups of individuals. For instance, let’s imagine one is planning to develop and launch a novel audio-based system to recognise violent behaviours for the prevention of domestic abuse in households within the UK. The first problem a system developer may encounter is that not every household speaks English. A speech recognition model which is only trained with data from native speakers only, would certainly not perform well with data processed from non-native speakers. Additionally, there are other sound characteristics, such as tone, phonetics, intonation and melody which may vary considerably between different languages or even between different accents of the same language. Thus, although it may involve tedious processes of data collection, it is crucial to identify the target group and incorporate an adequate level of inter and intra-group variability when developing intelligent systems. This issue becomes even more crucial when dealing with sensitive matters like crime where false negatives can translate into serious personal health-related consequences.

Data Integrity

Data integrity refers to the consistency, accuracy and completeness over the entire life cycle of the different data retrieval, data transmission, data storage and data processing units of a system. Maintaining data integrity is crucial for various reasons. First, data integrity ensures recover-ability and trace-ability. Second, the decision-making made by intelligent systems is driven by the data it is developed upon, thus the accuracy of such systems strongly depends on the integrity of the data they are developed, maintained and functioned with.

Battery Life

Energy reduction and sustainability have become major issues in the technical and social agendas in the last years. The ubiquitous and pervasive computing research communities are systematically facing a strain between usability and sustainability. On the one hand, users express an increasing interest in purchasing more sustainable products. On the other hand, they do not wish to do so at the sacrifice of their comfort. The widespread use of mobile and portable devices such as smart-phones or tablets comes alongside an ever increasing demand for mobile apps, including resource demanding applications such as face, speech or activity recognition. Although resources like memory, bandwidth and processing power are constantly being improved to keep up with the increasing demand for additional storage, communication and processing power, battery capacity grows only at an approximate rate of 10% per year [88]. However, increasing battery capacity is not the only way to improve battery lifetime. Alternatively, research efforts have been and should still be made to explore ways to reduce power consumption from mobile devices

Accuracy and Experimental Constraints

Intuitive optimization of various parameters often result in better and more accurate models, with error rates being continuously lowered. However, there exist various limitations and challenges which do not normally allow Artificial Intelligence (AI) applications to exhibit error-free performances. First, machine learning and deep learning algorithms typically require large amounts of data to successfully undergo the training phase. In addition, as mentioned in Section 4.3, such data should incorporate the adequate inter and intra-subject variability for the classification or regression models to be able to generalize well on unseen data samples. This means that in addition to the need to collect large amounts of data, that data has to be variable enough to adequately represent the characteristics of the target population and avoid large generalization or out-of-sample errors. Further to ensuring the collection of "enough" data samples, adequate feature engineering and machine learning techniques can be a crucial factor to optimize the accuracy achieved by AI-based crime prevention systems. A research challenge therefore arises from the need to improve the performance achieved by the state-of-the-art in the corresponding fields. For instance, as a current survey on sentiment analysis indicates [89], the classification accuracy achieved by the state-of-the-art on sentiment analysis using audio recordings, is in the range of 72.9% to 85.1%. This means that if an audio-based verbal abuse system was to be developed, it would be wrong 14.9% of the cases.

Affordability

Cost was a key factor discussed during the focus group as end users and other supporting organisations would need the device to be as inexpensive as possible if it was to become adopted into practice. In this regard, while tagging technologies relatively cheap, applications requiring high processing power may depend upon expensive hardware. Edge computing enables processing all or part of the data at the location it is collected. Data that is only of ephemeral

importance can be crunched on the edge device itself. This is in contrast to cloud-based systems, where data is sent to large, remote data centers for processing. In accordance with Moore's Law [93], small devices at the edge have become more computationally powerful. If the trend is to continue, it is only inevitable that switching to edge platforms would offer much affordable solutions in the long run. This territorial proximity to the endpoint is good for both latency and efficiency as it saves networks from unnecessary congestion as well as from carrying sensitive personal data. The ongoing minimization and mass production of electronics has enabled a reduction in the cost of edge computing devices, whereby various complex computations (such as AI and data processing) can take place on-board. However, the more data and computing intensive an application is, the more data storage and processing power are required, with this having an impact on the price to be paid by end users. In this regard, the adoption of high processing power technologies by the public has two main research challenges associated to it. First, to keep up with the ongoing miniaturization and cost reduction of electronic components. And secondly, the optimization of signal processing and machine learning algorithms so these can be adopted utilizing a lower computing power.

Technology Misuse and Technology Literacy

Advancement in technologies enables law enforcement and voluntary services to support victims and reduce or prevent crimes. However, the increasing complexity and communication capabilities present in these technologies have also opened new pathways for data interference[94]. There is little empirical research published concerning the use of technology in intimate partner stalking, as most of the current efforts are focused on online abuse on social media or texting [95]. Within these, the work in [95] conducted a survey with 152 domestic violence advocates and 46 victims. The study found that modern technologies can potentially give perpetrators multiple tools to control and manipulate people and that technology-facilitated stalking needs to be treated as a serious offense. There is thus a need for non-judgemental responses from service providers and law enforcement to victims experiencing such abuse. As practitioners observed, advising victims to switch off devices, to withdraw from social media, or to change their profile or telephone numbers, is putting an enormous burden of responsibility on the victim to adjust their behaviour [96]. Additionally, disengagement from technology can mean that victims are increasingly uncontactable, which can impact the type and the timing of the support they receive from services. There is a great need to increase public awareness of the use of spyware to commit abuse and stalking. Likewise, law enforcement and victim support and rehabilitation organisations will benefit from learning about the latest development of technologies that might help vulnerable individuals or prevent technology misuse.

Conclusions and Directions for Future Work

Different technology-driven solutions and the potential adoption of contemporary smart pervasive, machine intelligence systems and miniature technologies for crime prevention have been considered and evaluated. As discussed above, in our view, there is enormous potential associated with the adoption of short-range communication technologies as a tool for crime

prevention. These technologies can be employed alongside current approaches, such as GPS monitoring, to provide a more robust proximity detection system, able to detect proximity in both indoor and outdoor environments. Smart and short-range tags could be employed to provide an instant access to information and also for emergency reporting. As discussed, several apps to report emergency situations and collect evidence of those situations have been developed in recent years. However, these apps commonly require the user to open the app and perform an specific action. 14 A PREPRINT - FEBRUARY 9, 2021 Furthermore, violence detection scenarios in home or work environments, the use of a audio-based technologies appear to be preferred against that of CCTV cameras given the ubiquity, spherical field and lower privacy concerns exhibited by the former systems. As exposed, the use of audio signal processing along with machine learning techniques, allowing for applications such as speaker idolization, speech recognition, person identification and sentiment analysis, could be key to identify violent language as well as violent actions. From a technical viewpoint, standalone systems employing a single sensing technology exhibit distinct limitations. However, the combination of technologies, can be of great use to identify violent scenarios, which can lead to the prevention of further occurrences and therefore to the ultimate prevention of criminal activity. In conclusion, not all circumstances or situations are the same and there will be no “one size fits all” solution(s). As such, it is important to explore the heterogeneity in offenders, victims, contexts of offending, and offending patterns to understand which solutions might work for whom, and under what circumstances. Beside privacy, scalability, affordability, miniaturization and personalization are some of the important factors that need to be considered when designing technologies for crime prevention. Nonetheless, future work will embody the conduct of focus groups with co-design and co-creation elements where the findings and conclusions drawn in this paper will be further discussed and analyses with end user organizations and various groups of interest. With this, we aim to gain more insights into the potential, limitations and drawbacks of the discussed technologies and obtain critical advise from experts in the field. The development and implementation of a number of prototypes of the selected crime prevention systems will follow.