Accepted Manuscript

Cognitive Checkpoint: Emerging Technologies for Biometric-Enabled Watchlist Screening

Svetlana N. Yanushkevich, Kelly W. Sundberg, Nathan W. Twyman, Richard M. Guest, Vlad P. Shmerko

PII: S0167-4048(19)30095-1
DOI: https://doi.org/10.1016/j.cose.2019.05.002
Reference: COSE 1525

To appear in: *Computers & Security*

Received date: 7 December 2018
Accepted date: 3 May 2019

Please cite this article as: Svetlana N. Yanushkevich, Kelly W. Sundberg, Nathan W. Twyman, Richard M. Guest, Vlad P. Shmerko, Cognitive Checkpoint: Emerging Technologies for Biometric-Enabled Watchlist Screening, *Computers & Security* (2019), doi: https://doi.org/10.1016/j.cose.2019.05.002

Cognitive Checkpoint: Emerging Technologies for Biometric-Enabled Watchlist Screening

Svetlana N. Yanushkevich, Kelly W. Sundberg, Nathan W. Twyman,
Richard M. Guest, and Vlad P. Shmerko

***Abstract*—This paper revisits the problem of individual risk assessment in the layered security model. It contributes to the concept of balancing security and privacy via cognitive-centric machine called an 'e-interviewer'. Cognitive checkpoint is a cyber-physical security frontier in mass-transit hubs that provides an automated screening using all types of identity (attributed, biometric, and biographical) from both physical and virtual worlds. We investigate how the development of the next generation of watchlist for rapid screening impacts a sensitive balancing mechanism between security and privacy. We identify directions of such an impact, trends in watchlist technologies, and propose ways to mitigate the potential risks.**

Keywords: Cognitive checkpoint, biometric-enabled watchlist, layered security, risks, modeling, privacy, mass-transit hubs, e-borders, e-interviewer, conflict resolving

I. Introduction

'Dr. Williams, we will need to speak with you in private, please come with me', asks the border officer by somber voice after examining Dr. Williams' passport. 'Why does this happen every time I travel', thinks Dr. Williams to himself while despondently following the border officer to the secondary-interview room.

Dr. Williams, a university professor who has never been in trouble with the law, complains that every time he travels, he is erroneously identified as being on the border-crossing watchlis, assumedly due to an unlucky coincidence. The unfortunate reality for Dr. Williams is that border officers are obligated to conduct a secondary-interview whenever a travelers name is identified as being a likely match on the watchlist. As a result, Dr. Williams, as with other travelers with a similar name, must endure the stress and anxiety of being mistaken as a watchlist target. Not only do travelers like Dr. Williams have the repeated annoyance and embarrassment of having to endure a secondary-interview every time they cross a border, they also risk missing flights or even having their traveling companions view them with suspicion. Regrettably, there are many similar situations when innocent persons are unnecessarily screened by border officers at airports, seaports, and land-crossings; a situation known as 'misidentification'. Simply put, 'misidentification' is when a person is initially matched to a name on a watchlist, yet upon closer examination, is found to not match the watchlist record.

Misidentification remains a common occurrence due to shortcomings in current watchlist technologies and provides the principal motivation for this paper. Contemporary checkpoint is a cyber-physical computational platform that includes traveler authentication [23], [29], [48] using e-passport/ID [5], watchlist screening [9], [51], [86], concealed object detection [32], [60], interviewing [1], [4], [61], and risk assessment [49], [74], [76], [78], [91] under umbrella of justice and privacy issues [10], [15], [19]. In the International Air Transport Association (IATA) roadmap [36], four pillars of the checkpoint of the future are identified: computation intelligence, operations, infrastructure, and economic measures. Self-service based on the intelligent human-machine and machine-machine interactions is the key trend in nowadays checkpoint design. The focus of this paper is biometric-enabled watchlist screening as a part of such checkpoint.

Watchlist screening is a mandatory mechanism of national and international security [10], [19], [29], [47]. In border crossing applications, a watchlist check aims to mitigate the risk that a 'persona non-grata' crosses the border [85], [86] . In essence, a watchlist provides a source by which various types of vulnerabilities ranging from traveler service inconvenience (wrong alarm) to allowing a person of interest to cross the border (impersonation attack) must be safeguarded against. Balancing privacy rights and expectations of individuals

S. Yanushkevich, and V. Shmerko are with Biometric Technology Laboratory, Department of Electrical and Computer Engineering, University of Calgary, Canada, Web: http://www.ucalgary.ca/btlab. E-mail: {syanshk,vshmerko}@ucalgary.ca. K. W. Sundberg is with Department of Economics, Justice, and Policy Studies, Mount Royal University, Canada, E-mail: ksundberg@mtroyal.ca. N. W. Twyman is with Missouri University of Science and Technology, U.S.A. E-mail: nathantwyman@mst.edu. R. M. Guest is with School of Engineering and Digital Arts, University of Kent, U.K., E-mail: R.M.Guest@kent.ac.uk.

with screening effectiveness is a human and machine performance challenge.

Fast-forward to future, Dr. Williams will interact with an intelligent biometric-enabled machine having the capability to identify him by more than just his name, ultimately making his travel experience less stressful, and the duties of border officers more effective, efficient, and focused. In this paper, we focus on capabilities of watchlist technology that would provide an appropriate balance between privacy and security. The core idea of our study is to integrate a biometric-enabled watchlist with an interview supporting machine, or 'e-interviewer'. In today's practice, the security and privacy issues of an biometric-enabled e-interviewer, from one side, and the non-biometric watchlist (A-watchlist) screening from another side, operate separately; that is, screening resources of e-interview are not being utilized for watchlist needs [61], [71], [82].

A biometric-enabled watchlist for rapid screening requires intelligent computing and a smart supporting infrastructure for the e-interviewer. It is technically reasonable to adopt the concept of e-interviewer for the purpose of the next generation of watchlist screening. We have designed, modeled, and prototyped this hybrid approach and observed that (a) security is improved, (b) the technology gap between current systems and the next system generation is decreased, and (c) the system cost is reduced [49], [50], [68], [82]. However, the privacy aspects of these solutions are more sophisticated compared to traditional approaches based on separation of traveler authentication, watchlist screening, and interviewing, and requires additional study, which is a central focus of this paper.

This paper is organized as follows. In Section II, related work is briefly reviewed. In Section III, we articulate the taxonomical overview of layered security; In Section IV, we describe the three core types of human identity; In Section V, we introduce the technical and privacy background of watchlist screening; In Section VI, we explain why contemporary watchlists pose risks; In Section VII, we identify why the rapid profiling in mass-transit hubs (i.e. airports and seaports) remains a challenge; In Section VIII, we offer a brief overview of achievements in screening technologies and describe their horizons; In Section IX, we illustrate a novel balancing mechanism between security and privacy for future generations of watchlists; and finally, in Section X, we summarize the results in the form of the conceptual trends.

II. Related work

A framework of the biometric-enabled watchlist screening using e-interviewer, in addition to traveler authentication, is comprised of deception detection mechanisms, spoken-dialog technology, and risk-assessment techniques. While the automated, biometric-based authentication is currently being deployed [25], the other components are at various development stages. Deception detection currently provides accuracy of 70%–77% when using facial image analysis [1], [88], and 52% when using voice-based clues [46]. Current technology gaps in the spoken-dialog machines are identified in review [93]. Those gaps include, in particular, absence of standard for testing and evaluation. An automated jurisdictional control of human-machine interactions, known as automated legal problem, is still an open problem, too [11]. Advanced biometric-enabled systems have been analyzed, in particular, in the following applications: 1) ambient intelligence systems [2], [21], [54]; 2) affect-aware computer applications [18]; 3) authentication machines [23], [48], and e-passports/ID technology [5]; 4) health, ambient intelligence, and security [26]. The key trend of e-borders is the integration of intelligent support at all levels of surveillance, control, and decision-making [25], [31], [36], [68]. Evidence accumulation and risk assessment machines are the critical components of this trend [29], [80]. They are mandatory in border crossing checkpoints, airports, and seaports, and are considered to be prospects for the future transportation systems and mass transit hubs [28]. In the area of risk assessment, significant progress has recently been reported in tasks such as watchlist check using surveillance face images [94], screening technology [73], and face verification from surveillance video frames [30].

III. Taxonomical overview of the watchlist layered security

We distinguish four levels of the watchlist technology, based on the Human-Human (H-H) and Human-Machine (H-M) interactions (Fig. 1):

Level I, – Non-automated classic H-H technology in which a border personnel assesses the traveler's risk using a list of names (Fig. 1-I). Any legislation problems and conflict situations are resolved by human.

Level II, – In the contemporary automated risk assessment, the traveler is profiled using the e-ID and a non-biometric watchlist (Fig. 1-II). Again, a human may be involved in resolving the legislation problems. This H-M technology is being used in multiple countries already [25], [29], [35], [48], [68].

Level III, – In the contemporary Pilot Projects, the e-interviewer evaluates the risks of deception [4], [61],

[71], [82] (Fig. 1-III). A non-biometric watchlist check can be added. Any legislation problems are being resolved by a human. This H-M technological level is compatible with levels I and II.

Level IV, – The proposed improvement of the e-interview performance (Fig. 1-IV) using a biometric-enabled watchlist and the automated jurisdictional control of the machine-generated questions called Conflict Resolver. Functions of the Conflict Resolver can be extended to provide legislation information for travelers.

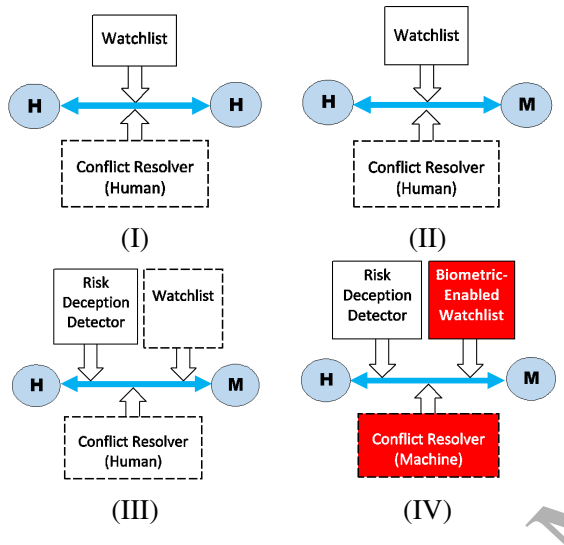

Fig. 1. Four evolutionary levels of the watchlist technology: (I) non-automated H-H interactions; (II) H-M interactions using the automated border control machines; (III) H-M interactions using an e-interviewer; (IV) H-M interactions assisted by a biometric-enabled Watchlist and a Conflict Resolver.

These levels of the watchlist technology correspond to a layered security paradigm. In practice, various combinations of layers have been proposed in order to improve security measures:

- The border personnel may not perform their task efficiently without automated assistance, thus, Level I does not satisfy the security requirements.
- Certain level of automation used at Level II provides some support in rapid traveler authentication but the watchlist remains non-biometric.
- At Level III, the e-interviewer technology assists in evaluating the risk of deception, however, a non-biometric watchlist is used.
- According to resent studies [49], [50], [91] using the biometric-enabled watchlists (Level IV) is imperative. This may, however, decrease the performance. This can be mitigated by: 1) integrating a biometric-enable watchlist in the e-interviewer based on the concept of intensive H-M cooperation, and 2) complimenting it with an additional control of H-M interactions using a conflict resolving mechanisms.

Biometric-enabled watchlist screening is the core of traveler risk assessment, and an integrated part of layered security. A special supporting infrastructure is needed to perform the clearance tasks. The term “layered security” also known as a “Swiss Cheese” model, addresses the security doctrine [16], [25], [78], [81] and its practical realization as a multi-state model [35], [59]. The idea of layered security is to distribute available resources (such as organizational topology, surveillance network, security personnel and service machines) in an optimal way in order to expedite traveler screening and service performance. A risk assessment of a given individual is an essential part of the layered security approach [25], [85], [86], [87], with the traveler risk assessment being a cornerstone of screening technologies. An example includes the US Department of Homeland Security (DHS) automated targeting system [19]. It was reported in [7], [23] that an automated border control (ABC) machine directed 8 out 100 (8.13%) travelers to the manual control because their names were on the watchlist. Geographical data of deployed ABC machines is periodically updated [37].

Fig. 2 provides a taxonomical view of a multi-state security checkpoint based on the traveler risk monitoring and control techniques including risk assessment, risk causal analysis, risk propagation, risk adjustment, risk fusion, risk reasoning, and risk prediction. Traveler’s risk is assessed using various mechanisms of forward risk propagation (a process from effect to causes), and backward risk propagation (a process from causes to effect) through the states. Risks states are adjusted using their causal relationships. This is the core principle of risk mitigation. Given a risk score and the state screening resources, a risk fusion results in a final decision. Biometric-enabled resources for the watchlist screening can be placed in one state, or distributed over several states. Formal aspects of some tasks, such as risk propagation, can be found in [22], and can be adopted, in particular, from multi-echelon supply chain problem [62], [70]. Other parts of the formalization of a multi-state screening model, such as risk mitigation, consensus of risk conflict assessments, and trust relationships between screening states, are commonly adopted from advanced group decision-making studies [8], [17], [56]. The value of the proposed taxonomical view (Fig. 2) is twofold:

1) This is a technology-independent model of any security checkpoint including four evolutionary levels of the watchlist technology (Fig. 1) which are implemented in one or a set of screening states

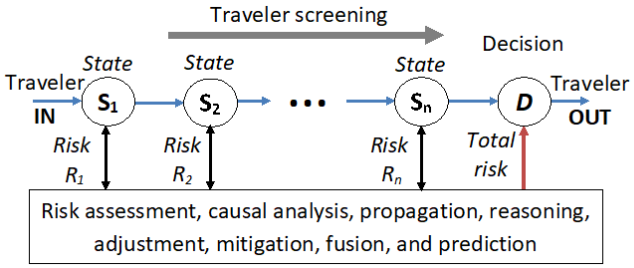

Fig. 2. Taxonomical view of multi-state security checkpoint.

2) This is a generalized model of a cognitive checkpoint which allows for local and global perception-action cycles and some necessary attributes of cognitive dynamical system [34].

Risk assessment resources are distributed in both physical and virtual/digital world. Layered security provides developers with the possibilities to mitigate against unwanted effects and/or emphasize attractive features of technologies, optimize security resources, manage risk costs and performance, as well as operations with degraded resources. In [39], the design goal is to minimize risks that "all the holes of a "Swiss Cheese" model do not line up". Some efforts to improve the performance of layered security have been reported with respect to: 1) topology of the waiting queuing lines [53] and checkpoint flow models [52]; 2) optimization of the passenger flows [64], [89]; 3) development of security measures [16], [78], including measures of the cost of travel time variability [24]; 4) cost-efficient minimization of security layers [77]; 5) modeling and simulation using a multi-state model of service [59], analytic hierarchy model [92] and hybrid models; for example, combining analytic hierarchy model and others, such as Dempster-Shafer [6], and Bayesian [58]; 6) traveler authentication and risk assessment, in particular, using multi-metric causal models [50], [91]; and cognitive agent models [45].

In these developments, different models of layered security for practical needs are demonstrated. For example, the conceptual models for risk assessment such as [78], provide useful information for a general vision of security infrastructure. In contrast, the model proposed by [59] reflects some particular aspects of traveler risk assessment.

The main requirement is to design a layered security structure in such manner that one layer compensates the limitations of another, and to discover the mechanisms that produce mutual reinforcement; the layers providing greater protection together compared to the sum of their individual effects [78]. For example: a) Efficiency of surveillance can be elevated via camera networking and their synchronization for tracking persons of interest, as well as integration of intelligent mechanisms [13], [20]; b) Performance of authentication can be improved via some preliminary traveler identification or recognition [50], and meta-recognition [72]; c) Performance of traveler risk assessment can be improved via a distributed pre-check mechanism [19], [25], [80]; d) Risks of attack can be mitigated via a specific space configuration and a topology of the queuing lines [53].

Rapid automation using human-machine and machine-machine interactions brings new possibilities in layered security methodologies, however these implementations often imbalance previously optimized security schemes [25], [29], [48], [76]. Our study focuses on these aspects and suggests a realistic cognitive model of traveler risk assessment (primary using biometric-enabled watchlist techniques) in the layered security infrastructure.

The mainstream in state-of-the-art layered security [10], [19], [25], as well as in long-term perspectives [36], [80], envisions the following characteristics of traveler authentication methods: 1) integration of authentication machines [5], [23], [48]; 2) prioritizing the self-service using intelligent spoken-dialog machines [93] and e-interviewer [1], [61], [82]; and 3) implementing traveler risk assessment using resources of both physical and virtual/digital worlds [50], [91].

Self-service in traveler authentication, and in other services, is implemented via a human-machine interaction in which the user cooperates with machine instead of another user who may be uncooperative (walking, talking, running user). Thanks to this fact, in any configuration of security layers, the machines for supporting self-service operations can be used as the source of traveler screening data. This suggests that interview supporting technologies should be integrated in these machines. From this perspective, our analysis delivers the following technology landscape: 1) Dynamical probabilistic models [64], [89]; they better reflect layered security properties; 2) Deep inference in traveler risk assessment [49]; 3) Predictive analytic and modeling including deep learning in traffic flow prediction [57]; 4) Traveler surveillance in physical world [10], [33], and virtual/digital world [9]; 5) Managing distributed resources [25]; 6) Attack countermeasures [5], [12], [14], [27]; 7) Technology gaps identification [36], [49], [80], including attack mitigation [63].

IV. Contribution

This paper contributes to the concept of layered security of mass-transit hubs such as airports and seaports.

Specifically, the study addresses the area of traveler risk assessment using cognitive computational platform that utilized a biometric-enabled watchlist technology. First of all, this paper provides the taxonomical vision of the watchlist technological landscape. Secondly, based on our experience in developments of biometric-enabled watchlist technology and e-interviewer techniques for rapid traveler screening, a key contribution of this paper is the identification of privacy risk factors introduced by future generations of watchlist screening, caused by automation. For mitigation of these risks, we propose:

1) A novel balancing mechanism between security and privacy; this mechanism is implemented via integration of the biometric-enabled watchlist functions into an e-interviewer; and

2) A novel intelligent privacy control of (a) machine-human interactions (the machine can generate legally incorrect questions), and (b) machine-machine interactions (machines can commit mistakes when operating with private data) for protecting a traveler's privacy; we call this a Conflict Resolver.

This paper also proposes an extension of terminology. In particular, in addition to coining the term 'Redress Complaint Disposition (RCD) metric', we propose the terms 'E-interviewer', 'Conflict Resolver', 'Privacy Gap', 'Data Life-Cycle Period', and 'Impersonation/Deception Risk Landscape' within the lexicon of those who engage in related research.

To the best of our knowledge, this paper is the first attempt to introduce future privacy concerns and considerations when developing next-generation watchlists based on the evaluation of technological gaps.

V. Three types of human identity and watchlists

Todays e-borders constitute one of the most significant and ambitious advancements in border management and security. E-borders include layered security that is achieved using both national and international standards, along with advanced authentication and risk assessment technologies that operate in compliance with privacy policy and law [15], [25], [35], [48]. Most countries around the world are involved in the e-borders project including the United States (US-VISIT), European Union (SmartBorders), Hong Kong, China (e-channels), Australia and New Zealand (SmartGate), Singapore (eIACS), and the United Arab Emirates (e-gates). Central to e-borders around the world is the use of watchlist screening as the core means to assess a traveler's risk.

Definition 1. *Three types of human identity are distinguished in watchlist technologies* [83]*:*

Type I: **Attributed** *(name, date and place of birth);*
Type II: **Biometric** *(such as face, iris, fingerprint, retina, gait, dynamic signature, and DNA profile); and*
Type III: **Biographical** *(life events including details of education, employment, marriage, mortgage, and property ownership).*

The human identity check is characterized by assessing risk of traits at every layer of security system. The layered security doctrine is a rational approach for identity check modeling and implementation:

- Attributed data of the ID verification must be supported by reliable biometric traits which represent evidence.
- Any potential attacks aiming at impersonation must be mitigated via biographical data,
- Risk of a wanted person mis-identification addresses the three components: attributed, biometric, and biographical data.

The ISO Standard [38] provides recommendations for the biometric-enabled border management using a watchlist. The following scenario is considered as an example. An individual is attempting to enter the United States. There is a watchlist hit, but there are no derogatory FBI IAFIS (Integrated Automated Fingerprint Identification System) records for the individual. This scenario is represented by the following basic flow of events: 1) An individual arrives at the border; 2) An officer scans the individual's machine-readable documentation; 3) The system locates a 2-print watchlist record for the individual based on the information entered (verify); 4) The officer sends the individual to a secondary inspection; 5) The system retrieves and displays to the Secondary Officer the individual's secondary view data, including the watchlist hit (retrieve data). 6) The secondary Officer captures the individual's 10 fingerprint images, and makes (and records) the entry decision. 7) The system links the decision and current encounter data to the individual's record (set biographic and biometric data).

Most contemporary watchlists use attributed data for the rapid screening of traveler who presents a passport or other identity document (as was the case in the earlier fictitious example using Dr. Williams) these are known as **A-watchlists**. More sophisticated watchlists use biometric data for the screening of visas that are affixed within a passport these are known as **B-watchlists**. In future generations of watchlists, all types of identity will be used. Lastly, biographical data is used when screening traveler during a more in-depth person-to-person secondary-interview these are known as **C-watchlists**. Notwithstanding contemporary

advancements in e-borders and watchlists, it is of critical importance to note that virtually every watchlist contains incomplete, erroneous, or outdated data.

For all e-borders watchlist screening programs, the analysis of human identity (attributed, and/or biometric, and/or biographical) is proceeded using verification/identification algorithms. In essence, human identity is 'checked' by reviewing a traveler's e-passport data against the watchlist. Then, if the traveler is verified to an acceptable degree of confidence as being 'trusted', they are permitted past the checkpoint. Conversely, if during identity analysis the e-border system identifies a traveler as likely being a person noted on the watchlist, border officers are alerted and the traveler is removed for secondary interviewing and examination. At each differing stage of the e-border screening process, privacy considerations are addressed to safeguard against having the travelers privacy and mobility rights violated.

Considering the importance accuracy plays within any e-borders system, in particular the importance of legal compliance and ensuring efficient, effective, and prompt border clearance it is of vital consideration that engineers and others involved in system design and operation take all reasonable and prudent steps to avoid watchlist data errors or omissions. Equally, those who are responsible for inputting data into e-borders systems must ensure they do so in a comprehensive, accurate, ethical, and legally compliant manner only using credible and confirmed information acquired through reliable sources. Lastly, certain processes must be in place to safeguard against duplicate data, missing and conflicting records, along with a rapid means to delete or otherwise correct data that is no longer valid, incorrect, or unconfirmed.

For example, the core of US-VISIT is the IDENT system that fulfills three security layers: 1) it confirms the identities of trusted travelers, 2) alerts law enforcement if a traveler's ID invokes derogatory information, and 3) alerts agents when someone is using a different persona or biographic identity than in earlier DHS encounters [42].

While the vast majority of traveler screened by the CBP are quickly processed, there are nevertheless are some travelers who are erroneously believed to be a subject on the watchlist, resulting in them being subjected to secondary interviewing, physical search, and other enforcement processes.

Biometric identity sources are distinguished as *physiological* biometrics such as face, fingerprints, and iris; *behavioral* biometrics such as facial expressions, body dynamics, and voice, as well as group and crowd behavior; and *social* biometrics that utilize the fact that a growing portion of off-line and on-line human activities leave digital footprints in various databases and social media. Each of these sources is an essential component of traveler risk assessment when used in combination, the result being more effective and accurate border screening and processing.

VI. Fundamentals of the watchlist technology

Irrespective of the various watchlists that exit, there currently are no commonly agreed set of factors or standard on which to evaluate implementation and performance. Despite that lack of standardization, most national border security watchlists nevertheless share the same fundamentals of watchlist technology.

Definition 2. Watchlist *is defined as a mandatory mechanism of e-borders which enables the ability to identify individuals of interest using biometric modalities and related context information (Definition 1). The fundamental characteristics of watchlists are:*

$$\texttt{Watchlist} \equiv \begin{cases} \texttt{Data type;} \\ \texttt{Reliability of sources;} \\ \texttt{Credibility of information,} \end{cases}$$

where 'Data type' means non-biometric, biometric, or mixed.

The efficiency of any watchlist depends on these three characteristics [85]. Given a person of interest, the privacy gap in the watchlist refers to the risks of operational phases between biometric acquisition/placement and data deletion. This time interval is called the data life-cycle period.

The experience of developing and deployment of CAPPS (Computer-Assisted Passenger Pre-screening System) screening technology suggests that (a) the above characteristic package can be supported only partially by contemporary technologies, and (b) an efficient mechanism for updating should be developed [47].

There is a number of reasons a traveler may be stopped as a result of watchlist check: (a) watchlist matches, (b) misidentification as a person of interest, or (c) someone mistakenly included the traveler in the watchlist. As a result of the watchlist screening process, the travelers may complain that they were adversely affected and seeks redress. In most nations having e-borders, a redress process exists through which aggrieved travelers can log a complaint with the government agency responsible for border screening. In the US, the U.S. Terrorist Screening Center (TSC) established the Redress Complaint Disposition (RCD) to evaluate watchlist performance [85].

Definition 3. *The* **Redress Complaint Disposition (RCD)** *metric is defined as being a traveler complaint*

logged as the result of a traveler complaining about being erroneously stopped during the border crossing process seeking some form of redress for this error. In the RCD-metric, the traveler can be in one of the following states [85]*:*

$$\texttt{Traveler} \equiv \begin{cases} \texttt{Non-related;} \\ \texttt{Positive match;} \\ \texttt{Misidentified.} \end{cases}$$

Unfortunately, each of these states can be a source of an incorrect decision. For example, 'Misidentified' means that the complainant, who is the subject of a terrorist-related screening but whose identity is not on the terrorist watchlist, is considered to have been misidentified because of name, date of birth, or passport number similarity.

The watchlist check impacts the border clearance performance such as the overall performance, which is defined as the *throughput* (number of travelers served per hour), as well as the *operational reject rate*, which is expressed by the clause "one in N travelers $(1 : N)$ is wrongly directed to manual authentication". Efficiency of the watchlist screening and related privacy indicators are measured via a set of parameters, in particular, the number of misidentifications per/hour and number of redresses per/month. These factors impact the throughput and operational reject rate.

There are three sources of privacy impact which can be defined using distinct types of interactions: 1) H-H, when a border officer interacts with a traveler for the watchlist check, 2) H-M, when a machine uses both the traveler's ID and evidence for the watchlist check, and 3) M-M, when two or more machines cooperate in the process of the watchlist check.

In the recent study [50], criteria and taxonomy for watchlists was developed with a focus on mitigating the risk of impersonation. Impersonation effects have different meanings when relating security and privacy indicators in H-H and H-M interactions. For example, beautifying effects on facial attractiveness in social perception (H-H interactions) such as facial makeup, colored eye lenses and facial plastic surgery, in H-M interactions may be considered to be an attack on the recognition process (the intentional change of appearance, unlike aging which is an unintentional attack, a natural biological process).

The central problem of the watchlist technology is an *e-personation*, – the impersonation of another person or entity through electronic means. Impersonation leads to serious national threats. In these scenarios, the machine for traveler risk assessment can make wrong decisions because the data about the impersonated individual is gathered from the moment a ticket is purchased (including information such as financial records, phone records, and social media including e-mails, blog entries, and website searches), which then is analyzed for the purpose of traveler risk assessment and to monitor social threats (community-forming, terrorism, political organizing, or crime). Detecting impersonation in social media arguably is the most urgent of problems. In contemporary border crossing infrastructure, an e-interviewer aims to support a border officer in their interviewing of traveler. The e-interviewer is viewed as an affective cognitive system because it utilizes data derived from behavioral and emotional states. Though similar in purpose to a traditional police polygraph machine, the two technologies use much different strategies, methods, and measures. The goal of an e-interviewer is to generate a deception or risk likelihood. It is well documented that in order to achieve acceptable accuracy for the e-interviewer there needs to be an analysis and tracking of many differing modalities containing distinct indicators of potential deception. Given a set of questions, responses by an individual are measured using various biometric modalities. They form a modality-specific information content or risk deception landscape. In the e-interviewer, data acquisition is implemented via non-contact technologies using various modalities (acquisition framework) such as the heart rate and blood pressure (in particular, micro color facial changes caused by the heartbeat), vocal features, oculometric factors, respiratory functions, thermal features, and kinesic factors. Analysis and profiling of the risk of deception requires deep inference technology.

'OK, I know, I complained at least three times,' Williams notes, 'I understand that this is a typical case where the balanced scheme of the watchlist check is in favor of national security but not my privacy'.

VII. Why does the legacy watchlist pose risks?

Legacy watchlist practices are based on attributed identity (A-watchlist) and are today generally viewed as being ineffective [10], [85], [87]. Reflecting again on the fictional scenario of Dr. Williams, he is being detained at border checkpoints because his name and birthday are the same as someone listed on the watchlist; an obvious drawback of A-watchlist screening. In almost every such case, insufficient personal data can be identified as the root cause. To overcome this problem, the border officer must try to attain additional information that can be used to definitively distinguish the innocent traveler (Dr. Williams) with the person of interest noted on the

watchlist. `'We are sorry to inform you Dr. Williams, as long as we continue using this system where a person having your same name is listed, you will forever be directed to a secondary-interview when you seek to cross the border'.` Unfortunately, there is currently no way to overcome this inherent shortcoming of technology, except some particular scenarios such as introduced in ISO standard [38], as well as in [10], [42]. Our study highlights the need for a new watchlist paradigm.

VIII. Why watchlist is an open research issue?

The International Air Transport Association (IATA) developed the principles of automated authentication using e-passport [35] and introduced the future horizon [36]. Unfortunately, these breakthrough solutions for traveler authentication only partially address traveler risk assessment using the watchlist technology. There are two types of watchlist check procedures "strongly controlled" and "weakly controlled" each impacting security and privacy in differing ways.

The "strongly controlled" process assumes a satisfactory level of technical and management resources to provide reliable traveler authentication and risk assessment. An example is a consular affairs database that determines if a foreign national should be granted a visa to visit the country. We use the term "weakly controlled" to indicate the most difficult part of the watchlist check that addresses the weaknesses of contemporary biometric technologies. For example, typical sources of image degradation include harsh ambient illumination conditions, mug-shots of facial images taken from passports, low-quality imaging devices, image compression and down sampling, out-of-focus acquisition, device or transmission noise, and motion blur [44], [49], [50], [51].

Significant progress has been achieved in watchlist screening specific to Entry-Exit systems due in large part to high performance in biometric modalities [10], [42]. For example, the Consular Lookout and Support System (CLASS) is the watchlist screening system used by CBP officers in the United States when assessing traveler visas and passports [85], and the Visa Information System (VIS) used for Entry-Exit screening in the Europe Union [25]. While the aforementioned all provide examples of widely used and generally effective rapid watchlist screening within mass-transit environments, it is important to note that much more is still needed in the way of improving accuracy, usability, and speed. Advanced recognition techniques for dealing with low-quality images or other biometric samples cannot be used in practice because of low reliability. The above scenarios reflect the concern of growing volume of travelers across the world. For example, the IATA and the International Civil Aviation Organization (ICAO) predict that the number of international air traveler will grow at around 4.1% per year. Passenger numbers are expected to reach 7.3 billion by 2034, with each of these travelers needing to be checked again a watchlist (http://www.iata.org/pressroom/). The 2020+ horizon of future border automation is introduced by IATA in [36]. This roadmap predicts some breakthrough technological solutions in the near future, such as deep profiling and continuous risk assessment.

IX. What has been done and what is next?

Contemporary watchlist screening is a highly composite technology. It includes many parts with sophisticated sub-components such as recognition, identification, verification, profiling, risk assessment, checking the authenticity of the documents and biometric templates in e-passport/ID, prediction, conflict resolving, and decision making. In our approach, the keystones of watchlist hierarchy addresses the type of utilized identity within Definition 1, that is,

$$\texttt{Watchlist} \equiv \begin{cases} \texttt{A-watchlist (Data Type I);} \\ \texttt{B-watchlist (Data Type I,II);} \\ \texttt{C-watchlist (Data Type I-III)} \end{cases}$$

Security and privacy aspects of contemporary A- and B- watchlists are well studied and documented. Examples of such watchlists include the Interpol Terrorism Watch List (ITWL) which constitutes a list of fugitives and suspected terrorists, and the No-Fly List which constitutes a list of people who are not permitted to board commercial aircraft due to their involvement with terrorism and criminality. The forefront of contemporary watchlist technological developments includes the U.S. Department of Homeland Security (DHS)'s ADVISE machine, CAPPS, Secure Flight, Interagency Border Inspection System (IBIS), Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS) with search capabilities for fingerprints, faces, irises, palms, scars, marks, and tattoos, the U.S. Department of Defense's Automated Biometric Identification System (ABIS) [86], [87] as well as IATA's strategic vision [36] and technology horizon.

The aforementioned constitutes the current visions upon which future watchlist technology will emerge the C-watchlist in our hierarchy. Whereas the reliability of security indicators is being improved in the C-watchlist, the privacy impact becomes more complicated for assessment. This is caused by various factors such as imperfection of data and sources of information, algorithmic

drawbacks, performance of authentication tools, time-consuming conflict resolution situations, and potential thefts of private data. Each scenario taking these factors into account may not only offend the traveler (wrongly suspected as terrorists) but may also create a bottleneck situation favorable for terrorist attacks. This is a critical point of the balance between security and privacy, and the reason why the rapid traveler profiling is needed.

Bridging the technological gap between A- and B-watchlists from one side and C-watchlist from another side, results in a specific support infrastructure, and other mechanisms that are defined in our study as e-interviewer. The C-watchlist uses the sources from virtual world, such as identification of a person of interest in social media [9], physical world, and interviewing technologies (evidence).

Challenges and prospects of watchlist check technology for e-border applications are summarized in Table I. Overall,

1) Privacy issues define a new horizon of H-M interactions (deep human profiling) and M-M (manipulation with human personal data) interactions.

2) The package of technical challenges such as image recognition, data fusion, and others, reflect the contemporary trends in intelligent computation. However, breakthrough solutions are needed to satisfy the new requirements for authentication and risk assessment infrastructure.

3) The gold standard of the listed challenges is the power of inference and prediction technologies. These high priority technologies rely on progress in machine learning and automated privacy regulations/control.

X. Cognitive platform for balancing between security and privacy via e-interviewer

Each phase in the evolution of watchlist technology (that is, A-, B-, and C-type watchlists) upsets the balance between security and privacy. The B-watchlist provides more security benefits compared with A-watchlist, but it involves new privacy risks such as forgery of biometric traits via various type of attack. The next generation watchlist (C-watchlist), provides more reliable traveler screening, whilst introducing new privacy risks caused by gathering and processing biographical data (Type III in Definition 1) should be mitigated.

In this section, we propose a mechanism to improve the balance between security and privacy for this type of watchlist. Following the concept of interview supporting machine [61], [82] and recently reported results on predicting the lie/truth responses of interviews [1], [66], [71], we developed the e-interviewer with add-in C-watchlist. In such a machine, the following supporting computational resources shall be integrated: 1)a generator of interview question based on advances in spoken-dialog systems, 2) a controller of privacy issues called a Conflict Resolver, which operates in 3) an adaptive feedback loop.

From the taxonomical view point, e-interviewer is a particular kind of spoken dialog-machines, or chatbots (also known as chat-agents), such as Clever-bot, XiaoIce, and Alice [55], [75]. In contrast to chatbots, task-completion systems are designed for accomplishing specific tasks, such as intelligent personal assistants (IPAs), for example, Apple's Siri (https://www.apple.com/ios/siri/), Microsoft's Cortana (https://www.microsoft.com/en-us/cortana/), Google Assistant, Facebook M (https://developers.facebook.com/blog/post/2016/04/12/), and Amazon's Alexa (https://developer.amazon.com/alexa/). Technologies of the contemporary IPAs and trends are analyzed in [69]. In particular, assistance in the form of a passive response to user requests is replaced by proactive anticipation of the user needs, and provides in-time assistance (reminding of upcoming events and recommending a useful service). These and other spoken-dialog machines are based on the following cognitive criteria:

1) Computational intelligence that explores learning through H-M and M-M interactions.
2) Feedback principle that is a facilitator of computational intelligence, and
3) Complex reasoning based on machine learning and probabilistic reasoning mechanisms.

Conceptually, any cognitive dynamical system consists of four elements: perception-action cycle, memory, attention, and intelligence [34]. In cognitive checkpoint, perception-action cycle aims at maximizing information gain about the traveler evaluated using the observable data. There are three key components of the perception-action cycle of the cognitive checkpoint: 1) *Traveler* as a subject of multiple security measures in the supported infrastructure. 2) A *Screening actuator* that initializes execution of a security task or several security tasks such as authentication (e.g. e-ID), human-machine interactions provided by e-interviewer, risk assessment (e.g. biometric-enabled watchlist and multiple-source information gathering), and concealed object detection (e.g. weapon or dangerous items). 3) An *Evidence analyzer* that provides the feedback information to the screening actuator. For example, to complete authentication task, additional data is needed; the traveler's response to

TABLE I
CHALLENGES AND PROSPECTS OF WATCHLIST CHECK TECHNOLOGY FOR E-BORDER APPLICATIONS

Challenge	Impact on security and privacy, and required breakthrough solution
Privacy, human rights	Legality of 1) Biometric-based profiling (such as facial, iris, fingerprints, blood pressure, and gait traits, as well features of plastic surgery, and implants), behavioral profiling (signature, speech and facial response), mental facilities (measures of truthfulness, deception manners); 2) Interviewing technology that uses elements of interrogation techniques, benchmarks and standards; 3) Control of manipulation of personal data in M-M interactions; and 4) Concept of Conflict Resolver for protecting traveler privacy.
Interview technology	Spoken interview (or dialog) system for traveler authentication and risk assessment using physiological and behavioral data, as well as personal data from the digital world. Benchmarks and standards.
Reliability	Evaluating watchlist information in terms of quality and truthfulness. Metrics for the reliability of sources (such as "reliable", "cannot be judged", "usually reliable", "fairly reliable", and "unreliable"), and information credibility (such as "confirmed", "cannot be judged", "probably true", and "possibly true"). Attacks and countermeasures.
Efficiency	1) Impact on the border clearance performance such as the overall performance and operational rejection rate; 2) the number of mis-identifications per/hour, the number of redresses per/month.

the e-interviewer causes the next question; additional data is needed to complete the risk assessment; and additional actions are needed to finalize the concealed object detection (e.g. elicit information, via interview, about the orthopedic implants being initially detected as concealed items).

A generic information-centered, or conceptual, model of the e-interviewer is introduced in Fig. 3. The model implements the perception-action cycle, and consists of the following components:

Trait Detectors: comparing the evidence (biometric traits) and ground truth data to make decisions regarding a particular feature.

Watchlist: introduces authentication information of person of interest, including biometric traits. Mechanism gathering, processing, and sharing personal data is given Fig. 4.

Baseline Assessment: created at the prototyping and calibration phasesvia trait inference using precise measuring techniques. For example, the ground truth of pupil dilation is measured under special conditions using precise biomedical devices whilst the overall ground truth (baseline) can be measured using the electro-dermal activity and electro-encephalogram techniques.

Risk Inference: the deception features obtained by observing an interviewee are summarized in special manner including resolving the conflict situations. Also, the biometric features of interest from watchlist are compared against the evidence features.

Decision-Making: the machine makes a decision regarding the level of truthfulness of the interviewee

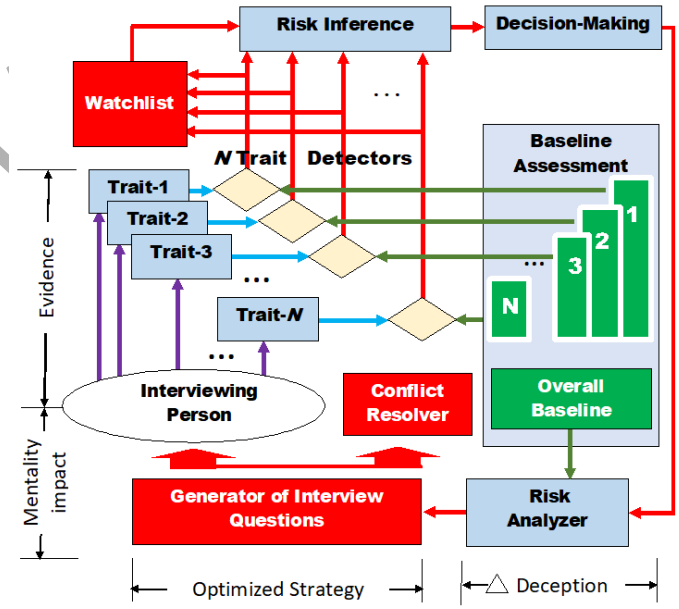

Fig. 3. Future generation of the e-interviewer for traveler authentication and risk assessment via watchlist check and interviewing. The model implements the perception-action cycle.

this level can be reassessed or confirmed by additional questions to the person.

Risk Analyzer: 1) it assess the deception risk as difference between the overall truth baseline and level of truthfulness, as measured, `<Deception risk, Δ> = <Overall truth baseline> – <Truthfulness>`; 2) it activates the questionnaire if

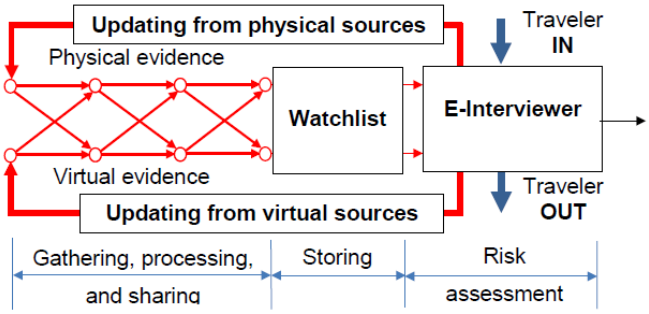

Fig. 4. Traveler risk assessment using biometric-enabled watchlist and e-interviewer.

features of a person of interest are detected.

Conflict Resolver: the aim of this component is a jurisdictional control of the questions that are generated, as well as attorney support to the interviewee if needed.

Generation of interview questions; generated questions and statements are systematized according to their impact on human mentality, cultural and social traditions, as well as security criteria.

E-interviewer operates as follows: (a) a traveler or interviewee is under observation using visual and acoustic sensors; (b) it is assumed the traveler also presents an e-ID to the machine; (c) a two channels screening process is employed: Channel 1 (which is hidden from the traveler) authenticates the travel documents, and then checks the traveler against available watchlists, and Channel 2 initiates the interview-based screening; (d) data from Channel 1 is transmitted to Channel 2 in order to provoke a question; (e) the response of the person being interviewed is measured using various biometric traits in comparison with the baseline assessment (ground truth); (f) deception risk inference results in both the deception risk landscape and decision-making based on the level of truthfulness; (g) the deception risk minimizer estimates the difference between the achieved and required level of truthfulness; (h) if the level is less than a given threshold value, the next question is generated; and (i) if the level is greater than a given threshold value the process is repeated according to the respective protocol.

XI. Cognitive Interview Management and Conflict Resolving Concept

Legal reasoning is the particular method of arguing used when applying legal rules to particular interactions among legal subjects, that is, human and machine in this paper. The key idea of automation of legal reasoning is to use the logic of legal texts, norms, and argumentation. Formal logic-based techniques are well suited for representation of legal rules, case facts, and for the inference that is based on the application of the rules to the facts [65], [67], [93].

An Conflict Resolver uses the text-mining to automatically profile and extract arguments from legal cases of border crossing interviews. Text-mining is well known in justice where case law plays a critical role in legal reasoning and decision-making [90]. Case law is a corpus of decisions on cases which judges have made. Such corpus is extremely large; this fact is the reason for development of the automated text mining for legal professionals. In our project, the case base is relatively small since it stores a specific semantic contents that is not bounded by any strongly specified dialog scenarios.

Automation of legal reasoning is a well identified branch of computational intelligence. Emergence of the e-lawyer coincides with the development of tools and techniques for rapid, real-time processing of large data sets that represent traveler interviews under the given statutes of jurisdiction. Both data-centric and logic-based models can be used for this purpose. A gap between the domain expert and a knowledge modeler in terms of legal argumentation/reasoning have been studied, in particular, in [67]. This is a subject of a *controlled natural language* using legal terms, rules, facts and concepts. A *legal landscape* is defined in [11] as a global characterization of the state of the law relevant to a given set of tasks. Examples include the automated techniques for legal patent, tax, and intellectual property landscaping, as well interview landscaping (related to this study).

In practice, various kinds of uncertainty impact the deterministic nature of formal logic. This is the main reason to resort to probabilistic techniques. An overview of reasoning-based legal techniques is given in [65], including probabilistic models of legal proof. It should be mentioned that jurisdictional support to travelers is of great demand in e-borders, and shall be incorporated in both the e-lawyer and e-interviewer. This is, however, is outside of the scope of this paper.

There are two levels of the H-M interaction control: 1) a traditional interview management concerned with contextual information, and 2) a juridical conclusion on the automatically generated questions implemented by the Conflict Resolver. In the interview management, the Conflict Resolver handles the following question-generation process:

$$\texttt{Conflict Resolver} \equiv \begin{cases} \texttt{Inaccuracy detection;} \\ \texttt{Inaccuracy prediction;} \\ \texttt{Inaccuracy recovery.} \end{cases}$$

The Conflict Resolver monitors the generated questions to assess whether inaccuracy has occurred. For example, if an inaccuracy is detected, the interview should be re-

covered via a strategically developed process. Details can be found in [93]. Technically, the interview management is an adaptive intelligent system.

Definition 4. *The* **Conflict Resolver** *is defined as an intelligence-enabled and mandatory component of the e-interviewer. The Conflict Resolver function is twofold: 1) to make the juridical conclusion on the automatically generated questions, and if needed, to block incorrect questions; and 2) if needed or otherwise appropriate, provide attorney support to the traveler.*

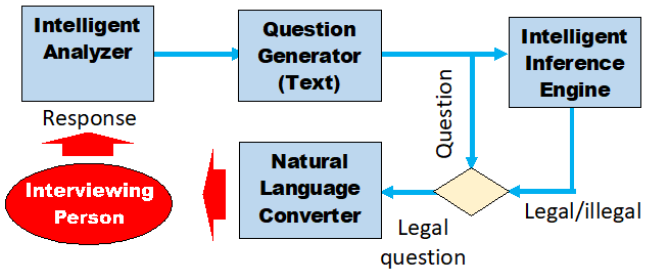

Fig. 5. The core of Conflict Resolver: architecture for a conversational legal reasoning system

In Fig. 5, the interviewee is placed in the question/answer loop where only legal questions are allowed. An automatically generated question (in the form of text) is analyzed by an intelligent inference engine. This results is the decision about legality of the question. The person's response, in natural language, is processed, and the decision on the next state is made. Note, that the content of the screening scenarios for any security applications can be well defined and formalized. From a general perspective, the Conflict Resolver should be integrated in any conversational legal reasoning system.

XII. Example of near future watchlist check

Ideally, three types of identity should be used in the watchlist as proposed in Definition 1. The question is how the machine processes this data. The answer is that the machine shall combine the functionality of both the contemporary authentication machine and the interview supporting machine. A possible (and realistic) interaction scenario can be as follows:

State 1: 'Good morning, Dr. Williams, what is the purpose of your trip?', a virtual border officer is greeting every traveler by name before starting any formal screening procedure.
Conflict Resolver: Proceed with the question.
*Comment:*Technically, it is possible because all travelers and visitors in the airport zone should be identified, tracked, and their risks should be continuously assessed.

State 2: 'Business. The only problem is with parking,' mumbles Dr. Williams, and hundreds of biometric traits such as voice pitch and facial expressions, are acquired and processed for estimation of the ground truth that is needed for further traveler response evaluation.

State 3: 'Sorry about that. Do not worry, your car is now in zone B103. Please, present your ID', asks the machine. Dr. Williams shows his ID, and the data (including his biometric traits) are scanned for processing.
Conflict Resolver: Proceed.

State 4: 'Mr. Williams, please put your luggage in the control box', the machine continues to accumulate the traveler data by fusing the risks of different items in the luggage.
Conflict Resolver: Proceed with the question.

State 5: 'Are you traveling with your spouse?", asks the virtual officer using information that has been sent by another machine.
Conflict Resolver: Proceed with the question.
Comment: This is an example of a machine constructed question that can be important for traveler risk assessment or other purposes. However, such a question risks intimidating subjects as it may appear that the computer somehow knows details about their personal relationships with others.

State 6: 'Yes, we are visiting our daughter,' states Dr. Williams, knowing that he must answer all the questions completely and truthfully adding, "She studies archeology at the university". At this time, the machine finishes the authentication process and starts the watchlist check.

State 7 (hidden) The machine formulates the question :* 'Is she married?' however before it is asked, it is evaluated by the Conflict Resolver.
Conflict Resolver: Dismiss this question.
Comment: In this last state, the question was dismissed by the Conflict Resolver due to it being irrelevant.

State 8 (hidden):* Again, the machine formulates another question 'Dr. Williams, is your right leg injured?', however before it is asked, it is also evaluated by the Conflict Resolver.
Conflict Resolver: Dismiss this question.
Comment: This is a conflicting scenario because the person of interest on the watchlist, Dr. Williams, has a record of being lame in the right leg.

State 9: The machine yet again formulates another question, 'Dr. Williams, did you have any limb injury?', and again before it is asked, it is evaluated by the Conflict Resolver.
Conflict Resolver: Proceed with the question.

Comment: The machine performs a comparison of all traits listed on the watchlist and the biometric-based evidence.

State 10: 'No, never, Im in good health and physical condition, and have been all my life', answers Dr. Williams.
Note: Conflicting situation is resolved, because the gait biometrics have not found any abnormality in the traveler's (Dr. Williams) gait.

State 11: 'Thank you Dr. Williams, you may proceed to the exit.'
Conflict Resolver: Proceed.

XIII. Generic trends as a summary

Watchlist screening is a routine security procedure that has been applied in one form or another for centuries. Today's reality provides the possibility for automated screening using all types of identity (attributed, biometric, and biographical) from both physical and virtual worlds. As noted, the primary aim of our study was to answer the question 'How the development of the next generation of watchlist for rapid screening can impact a sensitive balancing mechanism between security and privacy?' In this paper, we report the identified directions of such an impact, trends in watchlist technologies, and propose to mitigate the potential risks.

Trend A: **Delegating more privacy to machines.** Various new, unwanted effects can be expected, especially risky effects in M-M interactions. To mitigate the privacy impact in common practice, a general, yet internally accepted, security and privacy protocol is needed. The key idea of this protocol would be to shift the responsibility for storing personal data to its owner. Technically speaking, traveler biometric data are not stored in checkpoints (except watchlist) rather the data is stored in the traveler's e-passport/ID, resulting in the traveler having the care, control, and responsibility for their own e-documents. We follow this approach and propose a high-level control of H-M and M-M interactions via set of indicators such as content and relation to the task, that is, Conflict Resolver.

Trend B: **Increasing the depth of social embedding.** In feature watchlists, all types of identity data can be used for screening including traits from surveillance cameras and social networks (statistical surveillance). Considering this approach stands to increase the dimensions of privacy risks, it is recommended that a multi-biometric (e.g. in addition to facial recognition, the iris, and/or fingerprint) be included in the authentication process. We accept this common approach and propose the improvement via possibilities of H-M interactions on the cognitive platform of the e-interviewer.

Trend C: **Increasing the role of the behavioral and soft biometric.** This phenomenon addresses the need to increase the credibility of corresponding sources and supports the design of automated tools such as the e-interviewer. Following this trend and proposing the conceptual improvements to bolster the acceptance of the e-interviewer concept. This would unquestionably include steps focused on the balance between security and privacy.

Common to these trends is the cognitive platform. Further to proposing a cognitive approach to watchlist screening, this paper addresses H-M and M-M interactions in the form of an e-interviewer. The biometric-enabled watchlist as a part of cognitive checkpoint is closely related to forensics [40], [44], [50] and cyber-physical forensics [43].

Lastly, 'e-residency' based on the block chain technology [41], [79], and cloud computing [84] are two other relevant concepts that are subjects of future investigation in the ever changing layered security landscape.

Acknowledgments

This Project was partially supported by Natural Sciences and Engineering Research Council of Canada through grant "Biometric intelligent interfaces" and the Defense Research and Development Canada.

References

[1] M. Abouelenien, V. Perez-Rosas, R. Mihalcea, and M. Burzo, Detecting Deceptive Behavior via Integration of Discriminative Features From Multiple Modalities, *IEEE Trans. Inf. Forensic and Security*, vol. 12, no. 5, 2017, pp. 1042–1055.

[2] G. Acampora, D. J. Cook, P. Rashidi, and A. V. Vasilakos, A Survey on Ambient Intelligence in Healthcare, *Proceedings of the IEEE,* vol. 101, no. 12, 2013, pp. 2470–2494.

[3] T. Askeland, R. Flage, and T. Aven, Moving beyond probabilities Strength of knowledge characterizations applied to security, *Reliab. Eng. and Syst. Saf.,* vol. 159, 2017, pp. 196–205.

[4] AVATAR: Border patrol kiosk detects liars trying to enter U.S. *Homeland Security News Wire*, August 21, 2012. http://www.homelandsecuritynewswire.com/dr20120821-border-patrol-kiosk-detects-liars-trying-to-enter-u-s

[5] G. Avoine, A. Beaujeant, J. Hernandez-Castro, and L. Demay, A Survey of Security and Privacy Issues in ePassport Protocols, *ACM Comput. Surv.,* 2016, vol. 48, no. 3, Article 47, pp. 47:1–47:37.

[6] A. Awasthi and S. S. Chauhan, Using AHP and Dempster-Shafer theory for evaluating sustainable transport solutions, *Environ. Model. & Software*, vol. 26, 2011, pp. 787–796.

[7] D. Bachenheimer, Performance Measurement in ABC and Surveillance Scenarios, *Proc. Int. Biometric Performance Testing Conf.*, NIST, Gaithersburg, MD, 2014.

[8] T. Bedford, Decision Making for Group Risk Reduction: Dealing with Epistemic Uncertainty, *Risk Anal.,* vol. 33, no. 10, 2013, pp. 1884–1898.

[9] L. Best-Rowden, H. Han, C. Otto, B. Klare, and A. K. Jain, Unconstrained face recognition: identifying a person of interest from a media collection, *IEEE Trans. Inf. Forensics and Security,* vol. 9, no. 12, 2014, pp. 2144–2157.

[10] D. Bigo, et. al., Justice and Home Affairs Databases and a Smart Borders System at EU External Borders An Evaluation of Current and Forthcoming Proposals, *Centre for European Policy Studies (CEPS)*, No. 52/Dec. 2012.

[11] L. K. Branting, Data-centric and logic-based models for automated legal problem solving, *Artif. Intell. Law,* vol. 25, 2017, pp. 5–27.

[12] B. Biggio, G. Fumera, G. L. Marcialis, and F. Roli, Statistical meta-analysis of presentation attacks for secure multibiometric systems, *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 39, no. 3, 2017, pp. 562–575.

[13] P. Burgain, S. H. Kim, and E. Feron, Valuating Surface Surveillance Technology for Collaborative Multiple-Spot Control of Airport Departure Operations, *IEEE Trans. Intell. Transp. Syst.,* vol. 15, no. 2, 2014, pp. 710–722.

[14] J. D. Bustard, J. N. Carter, M. S. Nixon, A. Hadid, Measuring and mitigating targeted biometric impersonation, *IET Biom.,* , vol. 3, Issue 2, 2014, pp. 55–61.

[15] G. G. Clavell, Protect rights at automated borders *Nature,* vol. 543, Issue 7643, March, 2017.

[16] S. Chatterjee, S. C. Hora, and H. Rosoff, Portfolio Analysis of Layered Security Measures, *Risk Analysis,* vol. 35, no. 3, 2015, pp. 459–475.

[17] L.-C. Cheng, Y.-L. Chen, and Y.-C. Chiang, Identifying conflict patterns to reach a consensus - A novel group decision approach, *European J. Oper. Res.,* vol. 254, 2016, pp. 622–631.

[18] C. A. Corneanu, M. O. Simon, J. F. Cohn, and S. E. Guerrero, Survey on RGB, 3D, Thermal, and Multimodal Approaches for Facial Expression Recognition: History, Trends, and Affect-Related Applications, *IEEE Trans. Pattern Anal. and Mach. Intell.,* vol. 38, no. 8, 2016, pp. 1548–1568.

[19] Department of Homeland Security (DHS), Privacy Impact Assessment for the Automated Targeting System, DHS/CBP/PIA-006(b), 2012.

[20] S. P. Denman, T. Kleinschmidt, D. A. Ryan, et al., Automatic surveillance in transportation hubs: No longer just about catching the bad guy, *Expert Syst. with Appl.*, vol.42, no. 24, 2015, pp. 9449–9467.

[21] N. Diaz-Rodriguez, M. P. Cuellar, J. Lilius, and M. D. Calvo-Flores, A Survey on Ontologies for Human Behavior Recognition, *ACM Computing Surveys,* vol. 46, no. 4, Article 43, 2014.

[22] D. Dubois, Representation, Propagation, and Decision Issues in Risk Analysis Under Incomplete Probabilistic Information, *Risk Analysis*, vol. 30, no. 3, 2010, pp.361–368.

[23] S. Eastwood, V. Shmerko, S. Yanushkevich, et al. Biometric-enabled authentication machines: A survey of open-set real-world applications, *IEEE Trans. Human-Machine Systems*, vol. 46 , no. 2, 2016, pp. 231–242.

[24] L. Engelson and M. Fosgerau, The cost of travel time variability: Three measures with properties, *Transp. Res., Part B,* vol. 91, 2016, pp. 555–564.

[25] European Union: Technical Study on Smart Borders, *EU, European Commission, Unit C.3 – Transeuropean Networks for Freedom and Security and Relations*, B-1049, Brussels, 2014.

[26] M. Faundez-Zanuy, et al., Biometric Applications Related to Human Beings: There is Life beyond Security, *Cogn. Comput.,*vol. 5, 2013, pp. 136–151.

[27] M. Ferrara, A. Franco, and D. Maltoni, Face Demorphing, *IEEE Trans. Inf. Forensics and Security,* vol. 13, no. 4, 2018, pp. 1008–1017.

[28] Fiondella, L., Gokhale, S.S., Lownes, N., Accorsi, M., Security and performance analysis of a passenger screening checkpoint for mass-transit systems, *Proc. IEEE Conf. Tech. for Homeland Security*, 2012, pp.312–318.

[29] Frontex: Best practice technical guidelines for automated border control (ABC) systems, *Research and Development Unit*, Warsaw, 2012.

[30] G. Goswami, M. Vatsa, and R. Singh, Face Verification via Learned Representation on Feature-Rich Video Frames, *IEEE Trans. Inf. Forensic and Security*, vol. 12, no. 7, pp. 1686–1698, 2017.

[31] P. Grother, G. Quinn, and M. Ngan, Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects, *National Institute of Standards and Technology (NIST)*, Report 8173, March 2017.

[32] S. W. Harmer, et al., A Review of Nonimaging Stand-Off Concealed Threat Detection with Millimeter-Wave Radar, *IEEE Microwave Magazin,* Feb. 2012, pp. 160–167.

[33] B. Hayes and M. Vermeulen, Borderline the EU's new border surveillance initiatives, *Heinrich Boll Foundation*, 2012.

[34] S. Haykin, *Cognitive Dynamic Systems (Perception-Action Cycle, Radar, and Radio)*, New York, Cambridge University Press, 2012.

[35] International Air Transport Association (IATA): Automated Border Control. Implementation Guide, 2015. https://www.iata.org/whatwedo/passenger/Documents/ABC-Implementation-Guide-2nd-Edition.pdf

[36] International Air Transport Association (IATA): Checkpoint of the future. Executive summary. 4th Proof. 2014. http://www.bing.com/search?q=iata%3A+Checkpoint+of+the+future.+ Executive+summary

[37] International Air Transport Association (IATA): Automated Border Control Map, 2017 [Online]. Available: http://www.iata.org/ whatwedo/passenger/Pages/automated-border-control.aspx

[38] ISO/IEC 30108-1:2015, Information technology Biometric Identity Assurance Services, Part 1: BIAS services, *International Organization for Standardization (ISO)*, 2015.

[39] B. A. Jackson and T. LaTourette, Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries, *J. Air Trans. Manag.* vol. 35, 2015, pp. 26–33.

[40] Jain, A. K., and A. Ross, Bridging the Gap: From Biometrics to Forensics, *Philosophical Transactions of the Royal Society B*, vol. 370, Issue 1674, 2015.

[41] A. Judmayer, N. Stifter, K. Krombholz, and E. R. Weippl, Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms, *Synthesis Lectures on Information Security, Privacy, and Trust*, 2017.

[42] J. Kephart, Biometric exit tracking. A feasible and cost-effective solution for foreign visitors traveling by air and sea, *Centre for immigration study*, 2013.

[43] P. Kieseberg, et al., Real-time Forensics through Endpoint Visibility, *Proc. Int. Conf. Digital Forensics & Cyber Crime*, 2017, pp. 1–14.

[44] S. J. Klum, H. Han, B. F. Klare, and A. K. Jain, The FaceSketchID System: Matching Facial Composites to Mugshots, *IEEE Trans. Inf. Forensics and Security,* vol.9, no. 12, 2014, pp. 2248–2263.

[45] A. Knol, A. Sharpanskykh, and S. Janssen, Analyzing airport security checkpoint performance using cognitive agent models, *J. Air Transport Manag.*, vol. 75, 2019, pp. 39–50.

[46] G. Krishnamurthy, N. Majumder, S. Poria, and E. Cambria, A Deep Learning Approach for Multimodal Deception Detection, arXiv:1803.00344v1 [cs.CL] 1 Mar 2018

[47] W. J. Krouse and B. Elias, Terrorist Watchlist Checks and Air Passenger Prescreening, CRS Report RL33645 for Congress, 2009, https://fas.org/sgp/crs/homesec/RL33645.pdf

[48] R. D. Labati, A. Genovese, E. Munoz, et al.,Biometric Recognition in Automated Border Control: A Survey, *ACM Comput. Sur.*, vol. 49, no. 2, pp. 1–39, 2016.

[49] K. Lai, S. C. Eastwood, W. A. Shier, S. N. Yanushkevich, and V. P. Shmerko, Mass Evidence Accumulation and Traveler Risk Scoring Engine in e-Border Infrastructure, *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 10, 2018, pp. 3271–3281.

[50] K. Lai, S. Yanushkevich, V. Shmerko, and S. Eastwood, Bridging the Gap Between Forensics and Biometric-Enabled Watchlists for e-Borders, *IEEE Computational Intelligence Magazine*, vol. 12, no. 1, 2017, pp. 17–28.

[51] K. Lai, O. Kanich, M. Dvorak, M. Drahansky, et al. Biometric-Enabled Watchlists Technology, *IET Biometrics*, vol. 7, issue 2, 2018, pp. 163–172.

[52] K. Leone and R. Liu, Improving airport security screening checkpoint operations in the US via paced system design, *J. Air Transp. Manag.*, vol. 17, 2011, pp. 62–67.

[53] Y. Li, X. Gao, Z. Xu, X. Zhou, Network-based queuing model for simulating passenger throughput at an airport security checkpoint, *J. Air Transp. Manag.*, vol. 66, 2018, pp. 13–24.

[54] R. Li, B. Lu, and K. D. McDonald-Maier, Cognitive assisted living ambient system: a survey, *Digital Communications and Networks,* vol. 1, 2015, 1, pp.229–252.

[55] B. Liu, et al., Content-Oriented User Modeling for Personalized Response Ranking in Chatbots, *IEEE/ACM Trans. Audio, Speech, and Lang. Proc.*, vol. 26, no. 1, 2018, pp. 122–133.

[56] B. Liu, et al., Large-scale group decision making model based on social network analysis: Trust relationship-based conflict detection and elimination, *European J. Oper. Res.,* vol. 275, 2019, pp. 737–754.

[57] Y. Lv, Y. Duan, W. Kang, Z. Li, and F-Y. Wang, Traffic Flow Prediction With Big Data: A Deep Learning Approach, *IEEE Trans. Intell. Transp. Syst.,* vol. 16, no. 2, 2015, pp. 865–873.

[58] J. M. Moreno-Jimenez, M. Salvador, P. Gargallo, and A. Altuzarra, Systemic decision making in AHP: a Bayesian approach, *Ann. Oper. Res.,* vol. 245, 2016, pp. 261–284.

[59] A. G. Nikolaev, A. J. Lee, and S. H. Jacobson, Optimal Aviation Security Screening Strategies With Dynamic Passenger Risk Updates, *IEEE Trans. Intell. Transp. Sys.*, vol. 13, no. 1, 2012, pp. 203–212.

[60] N. Nikolova and T. Thayaparan, Ultra-Wideband (UWB) high-resolution radar for concealed weapon detection, Technical Report TR 2013-160, Defence Research and Development Canada, 2014.

[61] J. F. Nunamaker, Jr. D. C. Derrick, A. C. Elkins, J. K. Burgoon, and M. W. Patton, Embodied conversational agent-based kiosk for automated interviewing, *J. Manag. Inf. Syst.,* vol. 28, no. 1, 2011, pp. 17–48.

[62] A. Qazi, A. Dickson, J. Quigley, B. Gaudenzi, Supply chain risk network management: A Bayesian belief network and expected utility based approach for managing supply chain risks, *Int. J. Production Economics*, vol. 196, 2018, pp. 24–42.

[63] L. ben Othmane, R. Ranchal, R. Fernando, B. Bhargava, and E. Bodden, Incorporating attacker capabilities in risk estimation and mitigation, *Computers & Security*, vol. 51, pp. 41–61, Jun. 2015.

[64] J. Pitchforth, P. Wu, C. Fookes, and K. Mengersen, Processing passengers efficiently: An analysis of airport processing times for international passengers, *J. Air Transp. Manag.*, vol. 49, 2015, pp. 35–45.

[65] H. Prakken and G. Sartor, Law and logic: a review from an argumentation perspective, *Artif. Intell.*, vol. 227, 2015, pp. 1–58.

[66] B. A. Rajoub and R. Zwiggelaar, Thermal Facial Analysis for Deception Detection *IEEE Trans. Inf. Forensics and Sec.,* vol. 9, no. 6, 2014, pp. 1015–1023.

[67] S. Ramakrishna, L. Gorski, and A. Paschke, A Dialogue between a Lawyer and Computer Scientist: The Evaluation of Knowledge Transformation from Legal Text to Computer-Readable Format, *App. Artif. Intell.*, vol. 30, no. 3, 2016, pp. 216–232.

[68] J. J. Robertson, R. M. Guest, S. J. Elliott, and K. OConnor, A Framework for Biometric and Interaction Performance Assessment of Automated Border Control Processes, *IEEE Trans. Human-Mach. Syst.,* vol. 47, no. 6, 2017, pp. 983–993.

[69] R. Sarikaya, The technology behind personal digital assistants – an overview of the system architecture and key components, *IEEE Signal Process. Mag.*, vol. 34, no. 1, 2017, pp. 67–81.

[70] K. P. Scheibe and J. Blackhurst, Supply chain disruption propagation: a systemic risk and normal accident theory perspective, *Int. J. Production Research*, 2018, vol. 56, no. 1-2, pp. 43–59.

[71] R. M. Schuetzler, G. M. Grimes, and J. S. Giboney, The effect of conversational agent skill on user behavior during deception, *Computers in Human Behavior*, vol. 97, 2019, pp. 250–259.

[72] W. J. Scheirer, A. Rocha, R. J. Micheals, and T. E. Boult, Meta-Recognition: The Theory and Practice of Recognition Score Analysis, *IEEE Trans. Pattern Anal. and Mach. Intell.*, vol. 33, no. 8, 2011, pp. 1689–1695.

[73] A. Sgroi, P. J. Flynn, K. Bowyer, and P. J. Phillips, Strong, Neutral, or Weak: Exploring the Impostor Score Distribution, *IEEE Trans. Inf. Forensic and Security*, vol. 10, no. 6, 2015, pp. 1207–1220.

[74] J. Shortridge, T. Aven, and S. Guikema, Risk assessment under deep uncertainty: A methodological comparison, *Reliab. Eng. and Syst. Saf.,* vol. 159, 2017, pp. 12–23.

[75] H.-Y. Shum X.-D. He, and D. Li, From Eliza to XiaoIce: challenges and opportunities with social chatbots, *Front. Inform. Technol. Electron. Eng.*, vol. 19, no. 1, 2018, pp. 10–26

[76] SITA: END-to-end border management: An integrated approach to passenger data collection, identity verification and risk management. 2012, http://www.sita.aero/file/8505

[77] J. Skorupski and P. Uchronski, Evaluation of the effectiveness of an airport passenger and baggage security screening system, *J. Air Transp. Manag.,* vol. 66, 2018, pp. 53–64.

[78] M. G. Stewart and J. Mueller, Risk and economic assessment of expedited passenger screening and TSA PreCheck, *J. Transp. Secur.*, vol. 10, 2017, pp. 1–22.

[79] C. Sullivana and E. Burg, E-residency and blockchain, *Computer Law & Security Review*, vol. 33, Issue 4, 2017, pp. 470–481.

[80] S. Trochu and O. Touret, Managing the border, smartly, *Proc. European Intell. and Security Inf. Conf.*, 2013, pp. 281–284.

[81] Transportation Security Administration, *Layers of Security,* 2013. Available at: http://www.tsa.gov/about-tsa/layerssecurity

[82] N. W. Twyman, P. B. Lowry, J. K. Burgon, and J. F. Nunamaker Jr, Autonomous Scientifically Controlled Screening Systems for Detecting Information Purposely Concealed by Individuals, *J. Manag. Inf. Syst.*, vol. 31, no. 3, 2014, pp. 106–137.

[83] U.K. Cabinet Office, Identity Fraud: a study, July 2002, http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf

[84] J. Ullrich, T. Szeby, J. Fabini, and E. R. Weippl, Network-Based Secret Communication in Clouds: A Survey, *IEEE Communications Surveys & Tutorials*, 2017, pp. 1112–1144.

[85] U.S. Department of Justice Office of the Inspector General, Follow-Up Audit of the Terrorist Screening Center, Sept. 2007.

[86] U.S. Government Accountability Office (GAO), Terrorist watchlist screening. Efforts to help reduce adverse effects on the public. Washington, D.C., GAO-06-1031, 2006.

[87] U.S. Government Accountability Office (GAO), Data mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks, Washington, D.C., GAO-07-293, 2007. http://www.gao.gov/new.items/d07293.pdf.

[88] L. Warmelink, A. Vrij, S. Mann, et al., Thermal Imaging as a Lie Detection Tool at Airports, *Law Hum. Behav.*, 2011, vol. 35, pp. 40–48

[89] P. P. -Y. Wu, J. Pitchforth, and K. Mengersen, A Hybrid Queue-based Bayesian Network framework for passenger facilitation modelling, *Transp. Res., Part C*, vol. 46, 2014, 247–260.

[90] A. Wyner, R. Mochales-Palau, M.-F. Moens, and D. Milward, Approaches to Text Mining Arguments from Legal Cases, In E. Francesconi *et al.* (Eds.): *Semantic Processing of Legal Texts*, Springer, 2010, pp. 60–79.

[91] S. Yanushkevich, S. Eastwood, M. Drahansky, V. Shmerko, Understanding and taxonomy of uncertainty in modeling, simulation, and risk profiling for border control automation, *J. Defense Modeling and Simulation: Applications, Methodology, Technology,* Special Issue on Model-Driven Paradigms for Integrated Approaches to Cyber Defense - Part I, vol.15, no. 1, 2018, pp. 95–109.

[92] K. E. Yoo and Y. C. Choi Analytic hierarchy process approach for identifying relative importance of factors to improve passenger security checks at airports, *J. Air Trans. Manag.*, vol. 12, 2006, pp. 135–142.

[93] S. Young, M. Gasic, B. Thomson, and J. D. Williams, POMDP-based Statistical Spoken Dialogue Systems: a Review, *Proc. IEEE,* vol. 101, no. 5, 2013, pp. 1160–1179.

[94] Y. Zhu, et al., Still-to-Video Face Matching Using Multiple Geodesic Flows, *IEEE Trans. Inf. Forensic and Security*, vol. 11, no. 12, pp. 2866–2875, 2016.