Smart TV Face Monitoring for Children Privacy

Patrick C. K. Hung[1,2], Kamen Kanev[1,3,4], Shih-Chia Huang[1,2], Farkhund Iqbal[1,5], Benjamin C. M. Fung[6]

[1] Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada
[2] Department of Electronic Engineering, National Taipei University of Technology, Taiwan
[3] Graduate School of Science and Technology, Shizuoka University, Japan
[4] Lassonde School of Engineering, York University, Canada
[5] College of Technological Innovation, Zayed University, UAE
[6] School of Information Studies, McGill University, Canada
patrick.hung@uoit.ca, kanev@rie.shizuoka.ac.jp, schuang@ntut.edu.tw
farkhund.iqbal@zu.ac.ae, ben.fung@mcgill.ca

Abstract

Many of the modern Television (TV) sets and digital TV set-top boxes are endowed with Smart TV capabilities. Those include computing and connectivity to online services such as video on demand, online games and even sports and healthcare. A lot of Smart TV devices also have built-in cameras, microphones and other sensors that provide for environmental monitoring and consequent context dependent feedback. Such Smart TV capabilities, however, can lead to privacy violations through unwanted tracking and user profiling by broadcasters and other service providers. There is a concern when underage users such as children who may not fully understand the concept of privacy are involved in using the Smart TV services. To address this issue, face recognition experiments were conducted with the IBM's Watson and the Microsoft's Face Application Programming Interface to reveal the potential of integrating facial recognition in future privacy aware Smart TV services.

Keywords: Smart TV, Children protection, Digital imaging, Face recognition, Age estimation, Privacy

1 Introduction

Smart TV provides computing capabilities and connectivity to online services, such as on-demand streaming media, interactive media and housekeeping and healthcare applications. Google Smart TV, which is based on Google Android, can be automated, for example, to perform complex computing applications [35]. Smart TV successfully blends in the user life patterns through its ability to extract context information from the surrounding environment and to react accordingly [9]. Environment perception is carried out through sensors on the device such as microphones, cameras, and others. With respect to such context information, perception is fundamental to the device's abilities to make timely and context-sensitive decisions. In this regard issues of the Smart TV's social context have been discussed in [18] touching upon: (1) how people would perceive the area where Smart TV is being used, (2) what expectations for privacy in a room with Smart TV would users have, and (3) how other people in the vicinity (e.g., within hearing range) of the Smart TV would feel.

While Smart TV is becoming increasingly popular, it is certainly bringing new privacy concerns and potential security risks to its users. Ghiglieri [10], for example, demonstrate how Smart TV can be used by broadcasters and neighbors to track users if no privacy protection system is instated. Data that is collected to personalize the experience with Smart TV often contains sensitive information that obviously needs to be kept private from unwanted third parties. Consequently, many users are concerned with what personal data is being collected and how it is managed in the context of Smart TV [34]. Personal behavioral data is particularly sensitive, as it can be used to infer a significant amount of confidential information about the user, such as movement and lifestyle patterns, workplace behavior and others [13]. Thus, it is important to account for the specific privacy concerns, laws and regulations with respect to the Smart TV use. There is a concern when underage users such as children who may not fully understand the concept of privacy are involved in using the Smart TV services. In this study, we consider digital imaging-based methods for identifying and properly tagging children faces as a means to prevent unwanted disclosure of personal information. We carried out a series of experiments to evaluate the effectiveness of existing facial recognition technologies with respect to Smart TV. More specifically, experimental recognition of child face

*Corresponding Author: Patrick C. K. Hung; E-mail: patrick.hung@uoit.ca
DOI: 10.3966/160792642018091905029

presence in feedback image streams was conducted through the IBM's Watson and Microsoft's Face Application Programming Interface (API).

This paper continues with Section 2 covering related work and the corresponding literature. In Section 3 the concept of privacy policies is presented and discussed in detail. Section 4 reports on to the conducted experimental work and discusses the obtained experimental results. Finally, Section 5 draws some conclusions and outlines the plans for future work.

2 Related Work

Basic face recognition is typically carried out through standard pattern recognition methods. As a first step, test face images of different people are collected and registered to create a database for the face recognition system. The pattern recognition is carried out by analysis and comparison of the images in the database and the new test images supplied by the user. For better results, domain-specific enhancements of the employed pattern recognition techniques are often necessary. For example, Anggraini [1] proposes a method that uses Principal Component Analysis (PCA) and Self-Organizing Maps (SOM) for both feature extraction and clustering. With this method, the feature extraction gives access to the characteristics of the human while the clustering organizes the characteristics in sets and classifies them. Next, Horiuchi and Hada [15] discuss a face recognition technology that accounts for the face changes over the years, the face viewing angle, the different facial expressions and even for the accessories on the face. This technology targets elevated recognition precision and is applied to criminal investigations for evaluation of their accuracy. Another approach developed by Huang and Chen [16] uses the Local Vector Pattern (LVP) feature to calculate the distances between a given input face image and each of the enrolled face images and this obtain all possible face candidates. Then, a feature-point Bilateral Recognition (BR) algorithm generates the final face recognition result.

The face recognition problem becomes even more challenging in the case of streaming video with partial face occlusions. Ragashe et al. [24], for example, employ canny edge, Viola-Jones Face Detection and AdaBoost learning algorithm for better face recognition accuracy under such conditions. Soldera et al. [30] on the other hand propose a method that can handle sparse and dense face image representations. The sparse representation helps compensate for landmark location uncertainties during face image feature extraction using interpolated landmarks leading to better accuracy with high-resolution color face images. Next, Xi et al. [33] propose a method for face recognition employing deep learning, named Local Binary Pattern Network (LBPNet), which achieves high recognition accuracy without resorting to costly model learning approaches on massive data. While most of the reviewed works focus on general face recognition, a few of them also address the specificities of face recognition in the context of Smart TV. Further, Lee et al. [19] employ face recognition methods for viewer authentication and securing interactions with Smart TV systems. Nguyen et al. [22] on the other hand report on a gaze detection method based on head pose estimation in smart TV environments.

With respect to privacy, while most users appreciate the value of targeted services in Smart TV, they also express concerns over how their data is collected and managed without their knowledge. Cherubini et al. [6], for example, identify privacy as a barrier to the wider adoption of mobile phone services. About 70% of the consumers stated that it was important to know exactly what personal information was being collected and shared [20], while 92% of the users expressed concerns about applications collecting personal information without their consent [14]. Mobile applications have adopted a countless number of services to better analyze context data and to provide custom services that will be of better value to users, based on what they are most likely to need. While allowing context data to be collected for services can prove to be of great benefit to users, there is an ongoing tradeoff between utility and privacy [5]. Many users do not even know that sensitive information is being stored, in some cases even after permission was explicitly denied or withdrawn by the user. This clearly goes against the privacy principle of obtaining user consent before collecting such information. Other discrepancies and possible privacy violations occur when unnecessary large volumes of detailed and highly accurate data are collected and stored for longer than needed periods of time. Such discrepancies often take place because most of the permission details with respect to information collection are buried in lengthy, default-enabled policies that users can hardly understand [25].

We follow by illustrating how privacy is addressed in the context of Samsung's Smart TV which is capable of facial recognition. Faces can be saved to "Samsung Accounts" which can be used to sign into personalized apps such as Skype and Facebook. The Samsung's privacy policy regarding the facial recognition feature state that it can be used as a supplementary security measure in addition to passwords. The Samsung's Smart TV also incorporates a "Kids Service" which filters and makes content suitable for children but its connection to facial recognition remains unclear [27]. We summarized in Tables 1 and 2 the results of our search for Android and iOS apps incorporating facial recognition that might be relevant to Smart TV.

Table 1. Google Play Apps

App Name	Developer	Brief Description
AppLock Face/Voice Recognition	Sensory TrulySecure	Facial and voice recognition technologies applied to make unauthorized access to an Android device more difficult.
Face Recognition	Lakshmanan Anbalagan	Experimental app using OpenCV's face recognition functions.
Face Recognition	SeakLeng	Facial recognition software capable of being trained to better recognize a person.
Face Recognition FastAccess	Sensible Vision, Inc.	Facial recognition technology applied to authorize access to saved passwords on Android devices.

Table 2. Apple App Store

App Name	Developer	Brief Description
BioID Facial Recognition Authentication	BioID GmbH	Facial recognition used as a biometric security feature for accessing iPhone devices.
Face Recognition FastAccess	Sensible Vision Inc.	Facial and voice recognition technologies applied to make unauthorized access to an iPhone device more difficult.

3 Privacy Policies

Privacy protection is often addressed by adopting privacy policies as ways to communicate to end users how their data is collected, managed, shared and retained. A privacy policy should include a standard description of what information is collected from users, for how long the information will be retained, what the information will be used for, whether and how the information will be shared with third parties and so on. Despite the progress in the field, however, to the best of our knowledge, there is no current standardization effort for a privacy protection policy with respect to Smart TV and especially for children. For example, Google Android-based Smart TV users constitute a large segment of the consumer population to market researchers that collect their personal data and usage patterns for targeted advertising [26]. Third party advertisers can further infer additional person related knowledge based on context information and thus build detailed behavioral profiles that may be used for unknown or unwanted purposes. Personal data can come in many forms including browsing history, friends list, location information etc. Other examples of relevant context information [28] may include verbal context, roles of communication partners, goals of the communication and involved individuals with respect to the social environment, as well as spatial, chemical and other characteristics of the physical surroundings. The gathered information may seem trivial and often may not be perceived as particularly sensitive by the user, but in practice, when properly processed it may reveal a lot of important personal details.

In Smart TV, personalized services are provided to the user based on context data collected and inferred from embedded sensors and other environment data both volunteered and observed. In addition, Smart TV often involves a networked environment, which introduces further user privacy and security concerns, particularly related to the context information the Smart TV is processing [29]. Determining the amount of information to collect often requires a tradeoff between disclosing sensitive data and receiving context-awareness services in Smart TV. To provide highly relevant services to the user, more personal and context information need to be collected, this, however, raises concerns about privacy. A service in Smart TV, for example, can be designed to send special promotions and coupons to users depending on what is relevant to them. To identify the most relevant promotions, such a service will need to collect certain context data related to user behavior as well as profiling information including age and gender. The application may even collect and retain historical data on the users to determine what they are likely to do at certain times and analyze earlier interactions with the application to confirm interest in previously served promotions. In this example, the more information is collected on the users, the more relevant services can be provided to them but nevertheless, users may not be comfortable with the level of data collected and inferred on them. An application knowing where you are and what you are likely to be doing at any given time raises not only privacy but also a security concern. That is why context data is at the core of privacy concerns with respect to Smart TV's applications. Smart TV's applications must operate in a controlled environment and must protect data and resources from other untrusted applications that may be running on the device. This is usually regulated by security and privacy rules stipulated in End User Level Agreement (EULA) format. Smart TVs, however, often run third-party services that could, intentionally or unintentionally, violate such safety policies.

Different countries and legislation have different laws for privacy protection, and there are also many international guidelines and industry regulations which outline privacy best practices. These laws and regulations can also differ depending on what type of information is being collected (e.g., health information), or who the users are (e.g., children under the age of 13). For example, the Personal Data Protection Bill is a data protection framework to govern the processing of all personal data processing and collecting in Brazil, which imposes data protection obligations and requirements on personal data [7]. In Japan, the Act on the Protection of Personal Information Act protects the

rights and interests of individuals with their personal information [2]. In the United Arab Emirates (UAE), Protection of Personal Data and Privacy provides for "freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with law" [8]. In Taiwan, the Personal Information Protection Act (PIPA) regulates the collection, processing and use of personal information and personal data from citizens or non-citizens by government and non-government entities. The PIPA requires notification before personal information is collected, processed or used [4]. On the other hand, Canada's privacy laws are outlined in the Personal Information Protection and Electronic Documentation Act (PIPEDA), which governs how personal information can be collected, used and disclosed in commercial business. PIPEDA is based on the 10 principles of privacy outlined in the Canadian Standards Association's (CSA) Model Code for the Protection of Personal Information [12], which has been recognized as a national standard as of 1996 [3]. This model code is representative of the principles of the privacy legislation in many countries, including the United States and the European Union. It also bears similarities to the Organization for Economic Cooperation and Development (OECD) Guidelines for the Protection of Privacy and Trans-Border Flows of Personal Data [23] which have been adopted by the member countries of the European Union [32].

With respect to privacy as discussed above, our research focuses on a technical framework for children facial recognition in the context of Smart TV. Referring to Figure 1, the children (users) may interact with Smart TV services, possibly with Smart Phones, in a physical and social environment. As Smart TV can collect and manipulate a variety of data such as text, picture, video, sound etc. the scope of its use is far more complex than traditional TVs, given that the users can be both adults and children in a shared physical and social environment. Note that in such an environment improper privacy setting may jeopardize the physical safety of children if, for example, sensitive information is leaked to child predators. This is pertinent to the data collected by Smart TV, which includes information about the users (e.g., pictures of the children face) and context information extracted from their physical and social environments (e.g., pictures of other humans, ambient video, and audio recordings, registration of environmental conditions and infrastructure properties etc.)

We believe that parental control functions would be best implemented as embedded Smart TV features that will enable parents to restrict the content their children can release to Smart TV. Note that such functionality is different from the standard parental control features embedded in traditional TVs and set-top boxes. Efficient access to this new functionality could be provided through a rich data visualization model (e.g.,

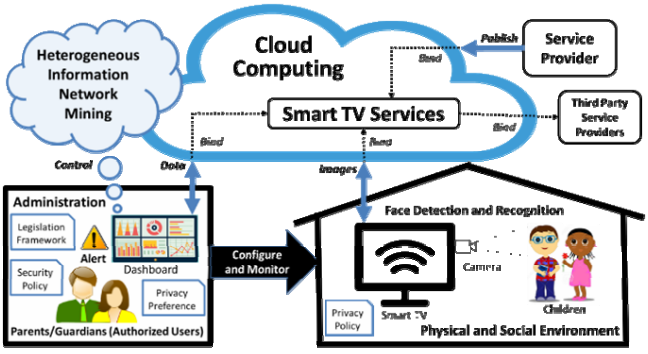

Figure 1. A conceptual view of the Smart TV privacy enhanced environment

supporting text, picture, video, sound, location and other sensing data) in the form of a dashboard for maintaining parental control through a common API for Smart TV service. The dashboard will also serve as an integration, validation and visualization tool for investigating and identifying privacy policies, preferences and specific rules applicable to Smart TV. A trusted third party (legal authority), who controls the enforcement of privacy rules in accordance with the United States Federal Trade Commission Children's Online Privacy Protection Act (COPPA) [31] may also be involved in this process. COPPA privacy protection of children under the age of 13, for example, stipulates that a child's personal information cannot be collected without parental consent. In 2010, an amendment to COPPA further elaborated that personal information includes geolocation information, photographs, and videos.

4 Experimental Results and Discussion

With this research, therefore, we aim to address the threats of information disclosure when children pictures are collected by current face recognition technologies. We have staged a set of experiments to explore the effectiveness of current face recognition technologies in the context of Smart TV and their possible application for detecting children faces in the collected feedback information. In this experiment, we assume that (1) the face recognition technologies store the face images in Cloud; and (2) the face images should be encrypted before outsourcing to Cloud storage for privacy requirements, which makes the traditional and efficient plain text keyword search technique useless [11]. Two facial recognition technologies were explored: IBM's Watson [17] and Microsoft's Face API [21]. Conducted experiments were organized in the following three stages: *Image Collection, Building Classification Model, and Applying Model for Face Classification* shown in Figure 2.

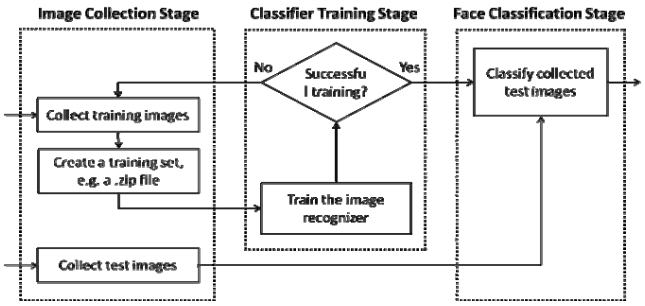

Figure 2. Experiment Stages

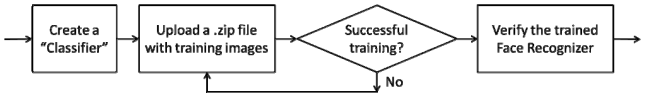

Figure 3. The process of training IBM's Watson API

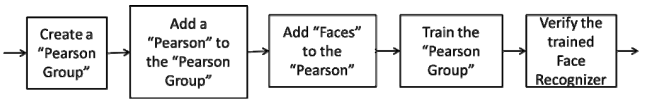

Figure 4. The process of training Microsoft's Face API

4.1 Face Based Age and Gender Detection Test

For this experiment, we used the existing image recognition demo data that was available with the employed recognizers, so no initial training was necessary. We tested the ability of the recognizers to provide gender and age feedback through recognition of 25 pictures of famous persons. The obtained results are summarized in Table 3.

Table 3. Experiment 1-Age and Gender Detection

Number of Images: 25		
	Positives	Negatives
IBM's Watson API	19/25	6/25
Microsoft's Face API	20/25	5/25

4.2 Recognition of Multiplicity of Facial Expressions with Felix Kjellberg

Images and videos of Felix Kjellberg, a popular comedy Youtuber was better known by his screen name "PewDiePie" are abundant on the Internet. The large variety of faces that he makes during his comedy shows provides a rich source of facial expressions suitable for testing and evaluating the accuracy of face recognition engines. For this experiment 180 online images of Mr. Kjellberg were collected and used for training of the two recognizers. Additional 20 images were collected and used for testing of the trained recognizers. The face of Mr. Kjellberg appeared in the test images at different angles and lighting conditions both alone and in a group with other people. After the successful training of both engines with the initial 180 images, Watson properly classified 4 and Microsoft's Face API 17 of the 20 test images (Table 4).

Table 4. Experiment 2A-Famous Youtuber

Number of "PewDiePie" Images: 20		
	Positives	Negatives
IBM's Watson API	4/20	16/20
Microsoft's Face API	17/20	3/20

Based on the demonstrated 85% face recognition success rate we deem Microsoft's Face API a suitable candidate for further experiments and implementation of face recognition in the context of Smart TV. The age of Mr. Kjellberg at the time of this writing was 26, and the ages estimated by the recognizer from his pictures were between 23 and 32. While this might be a promising result with respect to adult faces, further experiments will be necessary to clarify the suitability of the recognizer for age estimation of children faces. To conclude, we also tested 8 images of different people that look like Mr. Kjellberg. None of the look-alike's faces were mistaken for Mr. Kjellberg by either recognizer (Table 5).

Table 5. Experiment 2B-Look Alike Test

Number of "PewDiePie" Images: 8		
	Positives	Negatives
IBM's Watson API	0/8	8/8
Microsoft's Face API	0/8	8/8

4.3 Child to Adult Face Recognition with Macaulay Culkin

For this experiment, the face recognition engines were trained with a set of 141 images of Macaulay Culkin as a child (the boy from "Home Alone" movie series) collected from various online sources. Additional 20 images of the grown-up Macaulay were collected and used for testing after the training was completed. The relatively low recognition rates as shown in Table 6 are likely due to the significant changes that a child's face undergoes over just a few years.

Table 6. Experiment 3-Child to Adult

Number of Images with Macaulay Culkin: 20		
	Positives	Negatives
IBM's Watson API	2/20	18/*20*
Microsoft's Face API	12/20	8/20

5 Conclusion

Our studies clearly identified the increasing importance of privacy protection in the context of Smart TV and with respect to children and underage users. The experimental results show that the face recognition technologies may not be yet perfectly detecting a child's face.

Acknowledgments

This work was supported by the Ministry of Science and Technology (MOST), Taiwan, under MOST Grants: NTUT-KMITL-106-03, 105-2811-E-027-001, and 104-2221-E-027-020; the Research Office-Zayed University, Abu Dhabi, United Arab Emirates, under Research Projects: R15048 & R16083; the Natural Sciences and Engineering Research Council of Canada (NSERC), under Discovery Grants Program: RGPIN-2016-05023; and the Cooperative Research Project at Research Center of Biomedical Engineering with RIE Shizuoka University, Japan.

Special thanks to the technical contributions by Mr. David Mettrick, Faculty of Business and IT, University of Ontario Institute of Technology, Canada, the technical advice by Dr. Marcelo Fantinato, School of Arts, Sciences and Humanities, University of São Paulo, Brazil as well as the valuable suggestions by Dr. Panwit Tuwanut, Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang, Thailand and Dr. Yi-Hung Liu, Department of Mechanical Engineering, National Taipei University of Technology, Taiwan

References

[1] D. R. Anggraini, Face recognition using principal component analysis and self-organizing maps, *the 2014 Third ICT International Student Project Conference (ICT-ISPC)*, Mahidol University, Thailand, 2014, pp. 91-94.

[2] Cabinet Secretariat, *Act on the Protection of Personal Information Act No. 57 of (2003)*, Act No. 57, Japan, May, 2003.

[3] Consumer Measures Committee, Model Code for the Protection of Personal Information, the Office of Consumer Affairs Industry Canada, 1996.

[4] Ministry of Justice, *Personal Information Protection Act*, Laws & Regulations Database of The Republic of China, Taiwan, December 2015.

[5] S. Chakraborty, K. R. Raghavan, M. P. Johnson, and M. B. Srivastava, A framework for the context-aware privacy of sensor data on mobile systems, *the 14th Workshop on Mobile Computing Systems and Applications (ACM HotMobile2013)*, Jekyll Island, Georgia, USA, 2013, pp. 11: 1-11: 6.

[6] M. Cherubini, R. de Oliveira, A. Hiltunen, and N. Oliver, Barriers and bridges to the adoption of today's mobile phone contextual services, *the 13th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI'11)*, Stockholm, Sweden, 2011, pp. 167-176.

[7] J.-M. C. Brook, *Introduction to Privacy Law in Brazil*, CIPP Guideline, February 2015.

[8] K. Dearsley, B. Abouchakra, and J. Ryder, *DLA Piper's Data Protection Laws of the World-the United Arab Emirates*, UAE-Dubai (DIFC), January 2017.

[9] S. Wang, T. Lei, L. Zhang, C. H. Hsu, and F. Yang, Offloading Mobile Data Traffic for QoS-aware Service Provision in Vehicular Cyber-Physical Systems, *Future Generation Computer Systems*, Vol. 61, 2016, pp. 118-127.

[10] M. Ghiglieri, I know what you watched last Sunday: A new survey of privacy in HbbTV, *Workshop of Web 2.0 Security & Privacy 2014 in conjunction with the IEEE Symposium on Security and Privacy*, San Jose, California 2014, pp. 1-9.

[11] S. Wang, A. Zhou, C. H. Hsu, X. Xiao, and F. Yang, Provision of Data-intensive Services through Energy-and QoS-aware Virtual Machine Placement in National Cloud Data centers, *IEEE Transactions on Emerging Topics in Computing*, Vol. 4, No. 2, 2016, pp. 290-300.

[12] The Minister of Justice, *Personal Information Protection and Electronic Documents Act*, Government of Canada, 2000.

[13] M. R. Anawar, S. Wang, M. A. Zia, A. K. Jadoon, U. Akram, and S. Raza, Fog Computing: An Overview of Big IoT Data Analytics, *Wireless Communications and Mobile Computing*, Vol. 2018, 2018, pp. 1-22.

[14] GSMA, *User Perspectives on Mobile Privacy-Summary of Research Findings*, futuresight, 2011.

[15] T. Horiuchi and T. Hada, A complementary study for the evaluation of face recognition technology, *the 47th International Carnahan Conference on Security Technology (ICCST)*, Medellin, Colombia, 2013, pp. 1-5.

[16] Y. S. Huang and S. Y. Chen, A geometrical-model-based face recognition, *the IEEE International Conference on Image Processing (ICIP)*, Quebec City, Canada, 2015, pp. 3106-3110.

[17] IBM, *Visual Recognition*, IBM Watson Developer Cloud, 2017.

[18] S. Landau, What Was Samsung Thinking? *IEEE Security and Privacy Magazine*, Vol. 13, No. 3, 2015, pp. 3-4.

[19] S. H. Lee, M. K. Sohn, D. J. Kim, B. Kim, and H. Kim, Smart TV interaction system using face and hand gesture recognition, *the 2013 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, USA, 2013, pp. 173-174.

[20] Privacy in Mobile Apps initiative, *Global Privacy Report 2013*, MEF, 2013.

[21] Microsoft Cognitive Services, *Face API*, Microsoft Aizu, 2016.

[22] D. T. Nguyen, K. Y. Shin, W. O. Lee, C. Oh, H. Lee, and Y. Jeong, Gaze Detection Based on Head Pose Estimation in Smart TV, *the 2013 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, 2013, pp. 283-288.

[23] OCED, *The OECD Privacy Framework*, Organisation for Economic Cooperation and Development, 2013

[24] M. U. Ragashe, M. M. Goswami, and M. M. Raghuwanshi, Approach Towards Real Time Face Recognition in Streaming Video Under Partial Occlusion, *the 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, India, 2015, pp. 1-7.

[25] S. Wang, L. Huang, L. Sun, C. H. Hsu, and F. Yang, Efficient

and reliable service selection for heterogeneous distributed software systems, *Future Generation Computer Systems*, Vol. 74, 2017, pp. 158-167.

[26] D. Salomon, *Privacy and Trust in Elements of Computer Security*, Undergraduate Topics in Computer Science, Springer, 2010, pp. 273-290.

[27] Samsung, *Samsung Global Privacy Policy*, SmartTV Supplement, 2016.

[28] A. Schmidt, Interactive Context-Aware Systems Interacting with Ambient Intelligence, *Ambient Intelligence*, IOS Press, 2005, pp. 159-178.

[29] A. Shabtai, Y. Fledel, U. Kanonov, and C. Glezer, Google Android: A Comprehensive Security Assessment, *IEEE Security, and Privacy Magazine*, Vol. 8, No. 2, 2010, pp. 35-44.

[30] J. Soldera, C. A. R. Behaine, and J. Scharcanski, Customized Orthogonal Locality Preserving Projections with Soft-Margin Maximization for Face Recognition, *the IEEE Transactions on Instrumentation and Measurement*, Vol. 64, No. 9, 2015, pp. 2417-2426 .

[31] COPPA, *Children's Online Privacy Protection Act of 1998*, 15 U.S.C. 6501-6505, United States Federal Trade Commission, 1998.

[32] WIPO, *the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Directive 95/46/EC of the European Parliament and of the Council, 1995.

[33] M. Xi, L. Chen, D. Polajnar, and W. Tong, Local Binary Pattern Network: A Deep Learning Approach for Face Recognition, *the 2016 IEEE International Conference on Image Processing (ICIP)*, Phoenix, Arizona, USA, 2016, pp. 3224-3228.

[34] S. Wang, A. Zhou, W. Lei, Z. Yu, C. H. Hsu, and F. Yang, Enhanced User Context-aware Reputation Measurement of Multimedia Service, *ACM Transactions on Multimedia Computing, Communications and Applications*, Vol. 12, No. 4, 2016, pp. 1-18.

[35] M. Yusufov, I. Paramonov, and I. Timofeev, Medicine tracker for Smart TV, *the 14th Conference of Open Innovations Association (FRUCT)*, Helsinki, Finland, 2013, pp. 164-170.

Biographies

Patrick C. K. Hung is a Professor at the Faculty of Business and Information Technology in University of Ontario Institute of Technology, Canada. He currently works with Zayed University on cybersecurity research projects in the United Arab Emirates. His research interests include smart toys, robotic computing, services computing, and privacy.

Kamen Kanev has a Ph.D. in Computer Science from Sofia University in Bulgaria. He is currently a full professor at Shizuoka University in the Research Institute of Electronics. His research interests include Imaging and vision information processing; Patented Cluster Pattern Interface (CLUSPI); and Surface-based interaction models.

Shih-Chia Huang is a Professor with the Department of Electronic Engineering at National Taipei University of Technology, Taiwan. His research interests include intelligent multimedia systems, image processing and video coding, video surveillance systems, cloud computing and big data analytics and mobile applications and systems.

Farkhund Iqbal is an Associate Professor in the College of Technological Innovation at Zayed University. Previously, he worked as a Postdoctoral Research Fellow in the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec. His research contributions have been featured in both print and electronic media.

Benjamin Fung is a Canada Research Chair in Data Mining for Cybersecurity, an Associate Professor in the School of Information Studies, an Associate Member in the School of Computer Science at McGill University, a Co-curator of Cybersecurity in the World Economic Forum, and an Associate Editor of Elsevier Sustainable Cities and Society.