A Privacy Framework for Games & Interactive Media

Peter M. Corcoran, Claudia Costache
College of Engineeing & Informatics
National University of Ireland Galway
Galway, Ireland
peter.corcoran@nuigalway.ie

Abstract— Privacy is a concept that is intertwined with data security, but its scope is significantly broader. Often considerations of privacy in the context of consumer devices are limited to a consideration of the security of the data stored in those devices. In this work a broader perspective taken and privacy is defined in terms of new classes which consider the wider context of individuals and groups of persons. The implications for games & interactive media (G&IM) devices and systems is discussed. Finally, some ideas for an improved privacy framework for G&IM are outlined and explained in the context of the literature and current state-of-art.

Index Terms—Privacy, Games, Interactive Media, Wearables, Digital Media, Consumer Devices, Entertainment Devices.

I. Introduction & Context

Consumer devices today are de-facto connected to a network and invariably take advantage of a wide range of online services. The smartphone represents the pinacle of such devices but increasingly other consumer devices can now gather data in a persistent & continuous manner and thus data related to our behavioral traits, purchasing and consumption patterns, personal mobility, social groupings and individual lifestyle are increasingly exposed to government and corporations. It is unsurprising that the privacy of the individual has come to the fore in public forums and is a major concern for regulators and policy makers.

The recent introduction of the General Data Protection Regulations (GDPR) in Europe is one example of how government regulations are attempting to address the concerns of pervasive data harvesting. However, it must also be recognized that many of today's connected devices and associated consumer services rely on the individual consumer surrendering elements of their personal privacy in exchange for access to new services or conveniences.

In the context of Games & Interactive Media (G&IM) many of the general issues that arise with generic consumer devices are also evident, but in addition there can be a more intimate relationship between the creators of a digital gaming or interactive entertainment system and the players of these games. The players inhabiting an 'online world' influence and shape its growth and evolution. And as technology continues to evolve these virtual playgrounds become increasingly immersive for those who engage with them.

Our goal in this paper is to outline a framework that will allow both the provider and the consumer of an G&IM connected service to better understand what aspects of privacy such services might be infringing and outline what protections might be expected in return.

II. Related Works & Literature

In recent years there have been an increasing number of publications focusing on privacy for connected devices & services. Many of these focus on personal data [1]–[5], the need for a regulatory and legal framework [6]–[8] or the integrity of our computing devices and networks [9]–[11]. Typically a fairly narrow interpretation is given to the meaning of privacy – simply, that we should be in control of our personal data. In this work we take a broader perspective on what privacy means and consider not just data security, but the additional usage modalities of a connected G&IM device and associated network services.

The authors of [12] develop a 3-layer privacy responsibility framework, but this is largely concerned with aspects of data transfer. This work does not fully consider the complex use cases that can arise within online gaming or entertainment systems. Nevertheless many elements of their framework could be suitably extended. They introduce the key concepts of "privacy by policy" (involving mechanisms to provide the user with 'notice' and 'choice') and "privacy by architecture" (where privacy mechanisms are inherent in the system-level design). In [3] the authors identify 'profiling' of individuals as one of the most severe threats, particularly as business models that rely on this have demonstrated successes. They also note that the growth of 'Big Data' analysis techniques will drive further profiling activities. Several authors have discussed privacy design principles for interactive and ubiquitous systems. These include e.g. Langheinrich [13], Lederer et al. [14], Spiekermann and Langheinrich [15] and Clarke [16]. However these works pre-date the introduction of the multi-functional smartphone and tablets devices in use today and the recent growth in numbers of connected consumer devices and associated services.

In an earlier work [17] a privacy framework for IoT connected devices was proposed. Here this framework is reviewed in the context of G&IM devices & systems considering in particular the differences in typical gaming-related use cases, while noting the similarities & overlaps.

III. Classes of Privacy

To begin, it is useful to outline the main classes or dimensions of personal privacy [16], [18], [19].

A. Privacy of The Physical Person

This refers specifically to the privacy of the body. This class of privacy encompasses elements of biometrics, physically embedded devices such as RFID chips and physical implants

and extending to sensing devices designed to detect body signals. As one example, consider recent progress in technologies to directly interface with electrical signals in the brain. User interfaces that employ such technology introduce new privacy challenges related to the physical person.

B. Privacy of Behavior & Action

This class of privacy relates primarily to sensitive aspects of personal lifestyle. As examples it covers sexuality, religion, political and philosophical beliefs. Privacy is more difficult to quantify here as some individuals are more open and forthright in expressing these aspects of their life than others. Society itself can also strongly influence how this class of privacy is valued.

As a contemporary example, same-sex partnerships were not legally recognized in many countries until quite recently. As a consequence, individuals in such partnerships would have wished to keep their relationship private. The recent reversal of this practice in many jurisdictions will have changed the established social perception on such relationships and the importance of keeping such relationships private will now be less of a concern for many.

Infringement of this class of privacy can occur in different ways, ranging from profiling of the person to a direct interception of communications or data.

C. Privacy of Personal Communications

This class of privacy is exemplified by the classic 'wire-tap' on a phone call. From a legal perspective any privacy conversation or exchange of information through a physcial means such as a written letter or audio phone call is normally considered private between corresponding parties. But technological development has simplified, extended and commoditized personal communication through e-mail, mobile telephony and internet messaging to an extent where we generate hundreds of private messages on a daily basis. At the same time technology renders all of these communication mechanisms more vulnerable to interception than ever before.

In one quite recent example certain TV panels with voice actuation were designed to stream audio data to a network server to decode the received voice commands [20] – a clever engineering approach to reduce computational requirements on the device itself. Unfortunately, once this voice command mode was enabled audio data was continuously streamed over the internet and could be easily intercepted. In effect the TV became an internet-enabled bugging device that could spy on private conversations in your living room.

D. Privacy of Data & Image

This class of privacy was introduced by the authors of [18] primarily to cover the growing volume of image and video data generated by consumer devices and public surveillance systems. Every individual with a smartphone is now a well-equipped photo journalist and social media has created new distribution channels with high visibility for such data. In parallel, rapid advances in facial detection and recognition technology have commoditized the tracking of individuals in images and "Big Data" techniques enable the analysis of enormous image datasets and "profiling" of individuals on a scale that was simply not possible less than a decade ago. It is not difficult to see that new privacy challenges are created by this rapid evolution in technology and recent news scandals involving Camebridge Analytics and Facebook show how real and serious these challenges are.

E. Privacy of Thoughts & Feelings

Another 'new' class of privacy, again introduced with a view to reflect very recent developments in technology. A few years ago it was still possible to feel very comfortable in the privacy of one's own thoughts & feelings. Today this class of privacy is increasingly challenged by sophisticated monitoring technologies and advanced methods of data analysis. As examples, facial analysis can evaluate your emotions; voice analysis can detect stress levels and video analysis can detect and monitor blood flow in your face and extremities. Combining these, and other biometric signals & behavioral analysis cues enables aspects of our mental state to be predicted quite accurately. And today we are bringing new consumer devices such as 'smart speakers' into our homes – devices that are key actors in providing access to the raw data that can enable such predictions on a real-time basis.

F. Privacy of Location & Space

This overlaps to some degree with Data & Image privacy, but the focus here is on the loss of privacy in public spaces. Today, from local corner stores to airports, train stations and shopping malls we are exposed to constant surveillance. And where there is not a dedicated surveillance system you can be easily recorded on the images or video captured by others in a public space. The tracking of an individual via their consumer device(s) can also be considered as an aspect of this class of privacy.

With recent advances in drone technology the potential now exists to follow and observe an individual beyond fixed public surveillance networks and so the significance of this class of privacy continues to grow. There was a time when it was said that people came to the big city to hide in the crowd, but in a smart-city that will no longer be possible.

G. Privacy of Association & Group Membership

Privacy of association allows people of like mind to gather together and build communities, even when their views and philosophy is not mainstream. It is a freedom we expect in a progressive society. Today social media has enabled us to build communities more easily than in the past and to reach out and engage with audiences, small and large, sharing a similar perspective. The focus can be personal via a Facebook page, or more structured via Google+ or LinkedIn but the goal is similar - to build and gather like-mined groups of people.

For social media systems privacy and trust have become key components of their services. Some of these efforts were driven by EU legislation, but it is fair to say that a growing awareness among the user base of social media has led to a broad re-engineering in the past few years. Today social media infrastructure is increasingly sensitive to the user's need for control over the level of privacy associated with their activities. While it is not yet clear at what levels social media and IoT will interact there can be little doubt that the

widespread adoption of IoT will introduce some new challenges to user privacy in this area.

H. Privacy of Personal Experience

This last category of privacy was introduced by Clarke (http://www.rogerclarke.com/DV/Intro.html#Priv) to consider the growing trend to monitor a user's preferences when they access an online service, employing this information to learn about their personal preferences.

Consider as an example *Spotify* where samples of new music are offered to users based on their listening preferences. Arguably the user discovers new artists that they enjoy and most find this a helpful way to explore new music. But consider if this idea were applied to medical records to offer new experimental treatments for diseases – how would patients feel about such a service, even though it could offer significantly greater personal benefits than a music service? Although the underlying concept is almost identical the difference is that users are typically happy to declare their music preferences publicly, but not their medical history.

IV. Privacy Challenges for Games & Interactive Media

Gaming technology presents some interesting challenges from a privacy perspective when compared with other consumer technologies. Typically a user is constrained to use a game technology platform provided by the games manufacturer who can require access to personal information without the equivalent regularotry controls imposed in the financial or medical sectors. As most gaming platforms have evolved to become connected to the internet or some cloud services the potential for privacy issues is probably greater in the gaming sector than any other area.

It is helpful to consider some of the main gaming technology use cases.

A. Desktop & Console Based Online Gaming

Very few games are now created as stand-alone applications. There are too many advantages to linking a gaming system to the network and migrating certain elements of the gaming system onto cloud services. Connecting gaming clients to the cloud also opens the door to a wide range of multi-player and community enhancements that benefit the gaming experience and build user engagement and loyalty. As a result today's teenagers don't need to visit each other's houses after school to play games together – they can login and play together without leaving home!

However the game manufacturer typically has access to a users online activity and can monitor and analyze when and how they play games and who they play with. It doesn't take much consideration to realize the potential value of being able to track and monitor your users at this level of detail from their computer or gaming console.

B. Mobile Gaming

Mobile games today are almost as sophisticated as computer or console games and as a consequence are vulnerable to the same privacy issues. And given the versatility and sensing capabilities of modern mobiles devices there are additional concerns such as the capability to track the location of a user and access selfie images, facial data and even monitor a user's activity and health information.

Mobile devices are at the center of the battle for personal[i] privacy

C. Virtual Worlds & Communities

Modern games are often supported by substantial server & cloud infrastructure that enables many thousands of players to interact and engage with each other within the same gaming environment. For example *EVE Online* is a space-based, persistent world with more than 8,000 star systems built to support a massively multiplayer online role-playing game (MMORPG) where players can participate in a number of in-game professions and activities, including mining, piracy, manufacturing, trading, exploration, and combat (both player versus environment and player versus player). Eve Online appears to have peaked around 2013 with 0.5M active players. There are much larger communities – Wikipedia estimated *League of Legends* to have c.67 million players per month in 2014 and as of June 2018 *Fortnite* is estimated to have well in the order of 125 million active players.

And there are virtual worlds that are sufficiently sophisticated that they can be considered more versatile than a gaming enviroment. Linden Labs, 2nd Life peaked with slightly more than 1 million users around 2013 but still retains about 50% of those users, many of whom run virtual businesses within this virtual world and manage to earn a living. In fact 2nd Life has its own 'official' currency and supports a working virtual economy. It also has a privacy policy and tools designed specifically to give resident control over their privacy while online in 2nd Life.

D. Real-World Communities and eSports

The pervasiveness and popularity of online gaming environments coupled with the growth in connected technologies has led to the new phenomenon of eSports. In eSports highly skilled teams of players battle each other in a multi-player online battle area (MOBA) viewed by an audience of online spectators. The emergence of new streaming media platforms such as Panda.tv, Youtube and Twitch.tv has turned these online team battles into a rapidly growing online industry with an estimated 350+ million viewer audience in 2018. The same streaming platforms that enable audience participation and engagement with eSports also facilitate fans to group into online global communities. In a sense eSports is the 'new' soccer; its teams are formed from a global player pool and inspire fans and supporters from a global audience to band together to follow and cheer their team to victory. Much of this industry has grown from the availability of new scalable streaming platroms and still retains a sense of anarchy & non-conformity that appeals to its community. But as the eSports industry continues to grow it will need to self-regulate and the privacy and security of its community is a key area where attention is needed.

E. Virtual Reality & Immersion

Mobile, desktop, console and cloud gaming systems mirror today's mobile devices and cloud services so the privacy issues are broadly similar to those of, for example, Internet-of-

Things systems [17]. However when the introduction of Virtual Reality (VR) technology into connected gaming and interactive entertainment frameworks is considered it opens a whole new set of privacy concerns & challemges. Fully Immersive VR systems can blur the boudaries between the real and digital worlds. To achieve this they can, and indeed must seek frictionless transitions into the virtual worlds of online gaming communities.

Consider, as an example, the recent movie *Ready Player One* which shows the main characters seamlessly transitioning from their real-world selves into their digital counterparts. But there is no login process or no mechanism provided to prevent a different person entering and stealing an online persona? In contrast the movie provides significant details on 360 degree treadmills and haptic body suits. The reality is that advanced biometrics will likely be employed to create the seamless transitions required [21], [22]. But this will require the player of a gaming system to give the owner of a virtual world access to quite personal biometrics.

And perhaps a more disturbing thought is that as we spend more and more time in these engaging virtual worlds, and as the digitization of society continues to grow at an increasing rate, the digital assets that we hold in such virtual worlds may become more valuable and important to us than our real-world assets. Can we trust the owners and managers of these online worlds with essential elements of our growing digital presence – only time will tell.

F. Augmented Reality & Real-World Gaming

Interestingly, as VR begins to gain a significant foothold in gaming technology we see its 'little brother', augmented reality (AR) start to come of age. Mobile devices already have the applications frameworks via the introduction of ARkit [23] and ARcore [24] and we've seen the first breakthrough of AR technology in gaming space with the meteoric rise of Pokemon Go [25]. The open question is how long before AR moves from our devices and directly imposes itself onto our world-view?

While the first iteration of Google glass was abandoned [26] we have already been shown the way by digital pioneers like Steve Mann [27]–[30]. We can expect to shortly see a 2nd generation of "glass" that provides us with new AR windows on our surrounding reality.

V. Emerging Technologies for Games & Interactive Media

From the previous section, it is clear that several these classes of privacy are relatively 'new' and are introduced to correspond to the emerging challenges of today's technology, in particular connected devices with advanced imaging & display capabilities. These technologies have been evolving rapidly driven by the broad adoption of smartphones, the development of associated network technologies and more recently by emerging wearable display technologies.

Other challenges arise from the growth & proliferation of highly scalable streaming and videocasting technologies that enable individuals to share their personal gaming experiences in increasing detail with both active and passive participants. This section will focus on these two important areas where there are emering challenges.

A. Digital Streaming & Real-World Communities

Today's connected personal devices are much more capable than the desktop computer of 5-7 years ago. In addition to comparable computational power they incorporate a range of new sensing and communications technologies. When included in a mobile handheld device these capabilities raise many privacy concerns, but also enable the sharing and monetization of personalized experiences. The growth of youtube, twitch and discord based personal broadcast services are one example of how the smartphone has given rise to completely new experience-sharing modalities.

Image and Video: The video and image capture capabilities of these personal connected devices have evolved rapidly in terms of sophistication, and in parallel the growth of network infrastructure is driven by the demand for video services [31], [32], especially mobile-edge services for the latest high speed mobile networks [33]–[35].

Audio: Digital audio technology has also evolved but the complexities of rendering audio on consumer devices has posed challenges [36]–[38], but the emergence of new headphone technologies [38]–[40], audio objects [40], [41], spatially aware codecs [36], [41]–[43] and most recently synergies between embedded vision and audio rendering [44], [45] imply that we are on the brink of a new era of immersive spatial audio.

B. Augmented Reality Devices & Glasses

Today we see industry giant struggle with the maturing smartphone market – this segment can no longer offer growth and manufacturers are actively working to introduce the next 'must-have' consumer device. One clear candidate is an AR-display headset. Challenges remain as such a device must deliver on a compelling user-experience, coupled with a realistic battery-life and be presented in a lightweight and unobtrusive form factor. But most of the required technologies are sufficiently mature that we can expect a wave of such devices to launch in 2019 [46].

In turn we can expect these technologies will become a new growth driver for the gaming industry. In the same way that mobile devices drove an entirely new category of games and enabled completely new market segments a similar mini-revolution across the industry is to be expected with the introduction of AR gaming.

But as gaming and entertainment content gets Augmented it will also link into the real-world in ways that were not previously feasible. AR by its nature requires much more detailed knowledge of the surrounding environment and the people located in that environment and the veil of protection provided by a Virtual, computer generated, World is no longer available. In fact wearable Augmented Reality will present gaming and interactive entertainment technology with some of its greatest privacy challenges to date.

C. Biometrics & Personal Authentication

Today, biometric technology has become highly sophisticated and is widely available in various forms on smartphones [21], [22], [47], [48]. Fingerprint authentication

is available on many of the latest devices [49], [50] and we can expect additional biometric capabilities to become integrated with the next generation of devices [21], [22], [51]–[53]. These technologies will be available at low cost for new wearable and IoT systems and it will be a natural step for the next generation of wearable AR devices to incorporate biometrics to facilitate seamless user authentication.

But as our devices know who we are they can also reveal and share key biometric data with network and service providers. This raises a range of new privacy and personal data security issues. And as seamless authentication becomes a core service for gaming and interactive media technologies how can we address these new challenges? Next we outline and discuss a framework for addressing privacy issues in an increasingly connected and immersive digital world.

VI. Scoping a Framework for Systems Privacy in G&IM

The authors of [12] have introduced a three-sphere model of user privacy concerns and related it to system operations (data transfer, storage, and processing) through a responsibility framework. This is illustrated in overview by Fig1 below.

Sphere of Influence	User privacy concerns
User Sphere	• Unauthorized collection • Unauthorized execution • Exposure • Unwanted inflow of data
Joint Sphere	• Exposure • Reduced Judgment • Improper access • Unauthorized secondary use
Recipient sphere	• Internal unauthorized use • External unauthorized use • Improper access • Errors • Reduced judgment • Combining data

Fig 1: Three-Layer Privacy Responsibility Framework and Associated User Privacy Concerns reproduced from [12].

These authors also describe two approaches to engineering privacy: "privacy-by-policy" and "privacy-by-architecture." The first has a focus on implementation of the notice and choice principles of FIPs, while the architectural approach attempts to minimize collection of identifiable personal data and emphasizes anonymization and client-side data storage and processing. These are summarized in a responsibility framework, summarized in Fig 2 below.

The privacy-by-policy approach has been embraced by many businesses because it does not interfere with current business models that rely on extensive use of personal information. In the absence of enforced legal restrictions on the use of personal data, the privacy-by-policy approach relies on companies to provide accessible privacy information and meaningful privacy choices so that users can do business with the companies that meet their privacy expectations.

The privacy-by-architecture approach provides higher levels of privacy to users and without the need for them to analyze or negotiate privacy policies.

Approach to Privacy	Linkability of Data to Personal Identifiers	System Characteristics
By Policy	Linked by default	• unique identifiers across databases • contact information stored with profile information
By Policy	Linkable with reasonable & automatable effort	• no unique identifiers across databases • no common attributes across databases • contact information stored separately from profile and transaction information
Architecture	Not linkable with reasonable efforts	• no unique identifiers across databases • no common attributes across databases • random identifiers • contact information stored separately from profile and transaction information • collection of long-term personal characteristics with a low level of granularity • technically enforced deletion of profile details at regular intervals
Architecture	Unlinkable	• no collection of contact information • no collection of long-term personal characteristics • k-annonymity with large value for k

Fig 2: Privacy framework approaches & system characteristics, from [12].

Today we see some evolution in the practices of large corporations providing users with more choice and flexibility in how their personal data is shared, but much of the narrative around privacy still has a focus on user data. The key limitation of this responsibility framework is that it is focused on system operations - data transfer, storage, and processing – and envisages a well-defined system environment where the service provider is in control of both system & client behavior and the user is restricted in how they access and utilize the online service/system. It does not consider the rich additional data sensing and context metadata available from today's consumer device technologies and their applications in gaming & interactive media applictions and where these are integrated with wearable or network infrastructures. Nor does it consider the broader definition of privacy classes introduced here.

VII. New Challenges to Privacy

A. The Physical Person

The emergence of wearable and body area network (BAN) technology and its integration with gaming and interactive media technologies is creating a pervasive multi-device client eco-system. How should personal devices share data and sensor access? Should privacy be the responsibility of the device, or the BAN technology? Or we need a holistic multi-layered approach across BAN, LAN and WAN?

For biometrics an attacker could gain access to data through a variety of channels. Face and iris data can be harvested from images and videos. Video capable sensor nodes [54] could yield a rich harvest of biometric data. Data can be made available unintentionally if people opt to 'share' sensor feeds and of their experiences publicly or over local, insecure, channels. Practical protection against such attacks requires direct alteration of sensor data containing biometric components at the time of acquisition [55]–[57] or implementing a specialized network service to securely share sensor data [58], [59]. A related challenge is how to restrict a

3rd party from acquiring data in a public space in order to reverse-engineer biometric data. In such cases neither the end-user nor the service provider are involved in the data acquisition process and effective protection against such an attack is challenging, requiring a combination of advanced technical measures and a holistic approach to system services and data sharing policies.

B. Behavior & Action

Mobile and networked devices can harvest a wide range of location, behavioral and personal activity data and link these with an individual identity via biometric and transactional analysis. Such data may be used for innocent purposes, but it can also enable a detailed profiling of the individual that could easily reveal patterns of behavior & action that would be considered sensitive and private in nature. The increasing use of such devices in gaming and interactive media ecosystems introduces new challenges for tomorrows content developers. As one example, consider a participant in one of today's virtual worlds. Today, their virtual avatar may be anonymized, but in new ecosystems, as there is increasing integration between the 'real' and the 'virtual' it will become possible to associate the virtual avatar with 'real-world' transactions. Consider, as a simple use case, where virtual world services interact with the 'real-world' mobile device of the player. This information may be shared with/via 3rd parties, for example to enable music from a Spotify account to be integrated into the virtual environment. Now by associating virtual-world events & transactions with the timing of corresponding real-world transactions an attacker can determine associations between anonymized virtual avatars and real-world persons. In effect the real person can be profiled through their anonymous "virtual world" activities.

This form of challenge, personal profiling, was identified by the authors of [3] as a key privacy challenge. While their focus is on the Internet-of-Things we have shown that similar challenges exist for virtual worlds and associated G&IM technologies. Regulating access to such information is challenging as the sheer volume of online data associated both directly and indirectly with everyone continues to grow.

C. Personal Communications

The mechanisms of personal communications are well known and are individually covered by the framework of [12]. Here the challenge lies in the multiple modalities of communication employed by connected G&IM devices and the associated network infrastructures. Other authors have written in detail on Bluetooth [60], RFID [15], [61], [62], NFC [63]–[65] and GPS [66]–[68]. A key challenge is to manage the many communications and connectivity technologies used by connected G&IM in a holistic, open and transparent way.

D. Data & Image

In previous articles [69]–[71] I have written about the large volumes of images and videos that consumer devices are generating and how these devices have become the most active source of new online content. For many users more and more personal data is being sucked onto the cloud [72], [73]. But data in the cloud is exposed to additional privacy risks and has become a major focus for new social media and content-sharing services. Again there are new challenges [16], [74] lying outside the remit of a conventional privacy management framework.

E. Thoughts & Feelings

There is already a strong base of research on analyzing facial expressions [75]–[78]; more recently this has been extended to smartphone platforms [79], [80] and voice analysis provides an complimentary means to confirm the emotional state of the user. It would be quite practical to add blood flow pattern analysis [81], pupilometric [82], [83] and eye-gaze tracking data [84]–[87] using the front-camera of a state-of-art CE device. Indeed many of these technologies are being integrated into tomorrow's G&IM user interfaces and control systems. From a different perspective, AI engines have been at work for the last few years learning how to identify and implement voice queries [88]. The latest research focus for these engines is to incorporate knowledge of the emotional state of the user into the search query [89].

Thoughts, feelings and emotions are particularly exposed in G&IM environments – users enter virtual gaming worlds to escape from the 'real'; in doing so social norms and conventions are often disregarded. Thus, a user in a G&IM environment may behave in a manner that is unorthodox and even unacceptable in the 'real', yet the motivation for entering this framework is to obtain some escape from the 'real'. Here the question of privacy of thoughts & feelings becomes more important than in more conventional modes of interactions with connected technologies. After all, games are supposed to be 'fun', but where is the fun if you must moderate your in-game behaviors to match those of the 'real-world'?

F. Location & Space

As sensor networks become more prevalent and integrated into the fabric of buildings, vehicles and the surrounding urban infrastructure it becomes almost impossible to avoid being 'detected' and 'observed'. The core problem lies not with any single item of data that is generated by these pervasive connected device ecosystems and network infrastructures, but rather that by combining, analyzing and mining the rich data and metadata that will be generated it become feasible to track and monitor individuals with a degree of granularity that was not heretofore possible. Consider, for example, 5G technology which will bring Gigabit network speeds to mobile & wearable devices, vehicles and urban transportation systems. Key challenges will be how to preserve some degree of anonymity and privacy in such an environment of pervasive high-bandwidth connectivity. And more importantly to demonstrate & verify this in a transparent and credible manner

VIII. The General Data Protection Regulations (GDPR)

Maintaining a certain level of privacy in today's hyper-connected society is a massive challenge. There is no single approach to solve this enormous challenge, but it has now reached a point where public sentiment has begun to demand changes and government regulators are taking action [90]–[93].

In the context of social media and gaming, some efforts

have been made lately to allow users to maintain and even gain back control over the collection and usage of personal data by businesses and organizations. The most notable example of such efforts is the implementation of GDPR in EU on May 25th 2018 [94]. GDPR applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location and as a result it has forced businesses and organizations worldwide to re-asses their Data protection policies.

The new regulations aim to allow EU citizens better control of their data and also to increase obligations and accountability and to unify rules regarding usage of this data for businesses and organizations.

The main rights for users with regards to data privacy are outlined below:

Breach notification – the data controller is obligated to notify the users of any data breach that might result in a risk for the rights and freedoms of the user.

Right to access – the users have the right to know what personal data is being processed by the controller and for what purpose, and also to obtain a copy of the data collected by the controller

Right to erasure or Right to be forgotten – the user can request deletion of personal data by withdrawing consent or if the data is no longer relevant to original purpose for processing.

Data portability – the user can request personal data collected by a controller and transmit it to another controller

The main responsibilities for businesses are outlined below:

Data protection by design and data minimization: controller has the obligation to implement appropriate technical and organizational measures designed to implement data protection principles from the development stage of the applications, services and products and to ensure minimal processing of personal data collected.

Designation of a data protection officer - responsible for data protection, the DPO will be designated by public authorities and by businesses which process data on a large scale;

The controller is obliged to maintain a record of processing activities and to make these records available on request to supervisory authority.

Data protection impact assessment - businesses will have to carry out impact assessments when data processing may result in a high risk for the rights and freedoms of individuals;

Obtain clear consent from user – Consent should be given by an affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her

Processing of personal data should be lawful and fair - any information and communication relating to the processing of those personal data should be easily accessible and easy to understand, and clear and plain language be used (controllers should eliminate legalese from their terms and conditions)

In the context of connected devices, it is possible to identify a number of important measures that can contribute greatly to improved privacy protection for the individual.

IX. Elements of a Revised Responsibility Framework

There is no single approach to solve these enormous challenges, but it is possible to identify a number of important measures that can contribute greatly to improved privacy protection for the individual.

A. Privacy at the Edge

A simple principle – privacy issues should be addressed at the data source. In the context of IoT this implies that privacy sensitive data should be protected at the point of data creation. One example previously detailed, is to obfuscate sensitive biometric data in images at the point of acquisition. Other data may need to be preserved in its original form in which case it should be encrypted at source.

B. Privacy-aware Devices

As commented previously modern personal devices are prolific sources of many different kinds of data. Almost all of this data can be associated with some class of privacy risk and some risks can extend beyond the privacy of the user of the device. There is a strong mandate for an industry-wide set of guidelines for device manufacturers and sub-system suppliers. As IoT devices begin to proliferate online service providers should also engage with such efforts.

C. Broader Industry Co-operation and Awareness

Which leads nicely into our next point – there is a need for increased co-operation between the manufacturers of devices, components, and networking equipment, online service providers, standards bodies, infrastructure owners and public regulators to drive more privacy-transparent policies and architectural standards. Enforcing a privacy-friendly digital ecosystem should be everybody's business.

X. Concluding Remarks

Any new privacy framework for G&IM technology must take account of a much broader and more complex digital ecosystem. New data sources, online services and device functionalities have all to be considered. Sophisticated 'big data' tools will enable re-purposing and re-combining of data in novel ways. Increased sophistication in biometric analysis and personal profiling combined with growing smart-city infrastructures will make it easier to identify, track and monitor an individual.

Solving privacy in the coming decades is a grand challenge for industry, regulators and the public at large and the best balance will come from collaborative efforts involving all parties.

Acknowledgment

This research was funded under the Strategic Partnership Program of Science Foundation Ireland (SFI) and co-funded by SFI and FotoNation Ltd. Project ID: 13/SPP/I2868 on "*Next Generation Imaging for Smartphone and Embedded Platforms*".

References

[1] C. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," *The Internet of Things*, 2010.

[2] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, 2013.

[3] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: Threats and challenges," *Secur. Commun. Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[4] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Networks*, 2015.

[5] A. Samani, H. H. Ghenniwa, and A. Wahaishi, "Privacy in internet of things: A model and protection framework," in *Procedia Computer Science*, 2015, vol. 52, no. 1, pp. 606–613.

[6] R. Weber, "Internet of Things–New security and privacy challenges," *Comput. Law Secur. Rev.*, 2010.

[7] S. Peppet, "Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent," *Tex. L. Rev.*, 2014.

[8] R. H. Weber, "Internet of things: Privacy issues revisited," *Comput. Law Secur. Rev.*, vol. 31, no. 5, pp. 618–627, 2015.

[9] S. Tipton, D. W. II, C. Sershon, and Y. Choi, "iOS security and privacy: Authentication methods, permissions, and potential pitfalls with touch id," *Int. J. Comput. Inf. Technol.*, vol. 3, no. 3, pp. 482–489, 2014.

[10] S. Grzonkowski and P. Corcoran, "A privacy-enabled solution for sharing social data in ad-hoc mobile networks," *Consum. Electron. (ICCE), …*, 2011.

[11] D. Ferreira, V. Kostakos, and A. Beresford, "Securacy: an empirical investigation of Android applications' network usage, privacy and security," *Secur. Priv. …*, 2015.

[12] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Trans. Softw. Eng.*, vol. 35, no. 1, pp. 67–82, 2009.

[13] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," *UbiComp '02 Proc. 4th Int. Conf. Ubiquitous Comput.*, pp. 237–245, 2002.

[14] J. I. Hong, J. D. Ng, S. Lederer, and J. a. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems," *Proc. 2004 Conf. Des. Interact. Syst. Process. Pract. methods, Tech. - DIS '04*, p. 91, 2004.

[15] S. Spiekermann and M. Langheinrich, "An update on privacy in ubiquitous computing," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 389–390, 2009.

[16] D. Svantesson and R. Clarke, "Privacy and consumer risks in cloud computing," *Comput. Law Secur. Rev.*, vol. 26, no. 4, pp. 391–397, 2010.

[17] P. M. Corcoran, "A privacy framework for the Internet of Things," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp. 13–18.

[18] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European Data Protection: Coming of Age*, 2013, pp. 3–32.

[19] R. Clarke, "Intro. to dataveillance & information privacy; definitions of terms," *Roger Clarke's Dataveillance and Information Privacy*, 1999. [Online]. Available: http://www.cse.unsw.edu.au/~cs4920/resources/Roger-Clarke-Intro.pdf.

[20] S. Landau, "What Was Samsung Thinking?," *IEEE Secur. Priv.*, vol. 13, no. 3, pp. 3–4, 2015.

[21] P. Corcoran, "Biometrics and Consumer Electronics: A Brave New World or the Road to Dystopia?," *Consum. Electron. Mag. IEEE*, vol. 2, no. 2, pp. 22–33, 2013.

[22] P. Corcoran and C. Costache, "Biometric Technology and Smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts.," *IEEE Consum. Electron. Mag.*, vol. 5, no. 2, pp. 70–78, 2016.

[23] Apple, "ARKit - Apple Developer," *Apple*, 2017. .

[24] Google Developers, "ARCore Overview," *ARCore*, 2018. .

[25] BEN GILBERT, "Pokémon Go has been downloaded over 500 million times," *Business Insider*, 2016. .

[26] T. N. Y. Times, "Why Google Glass Broke," *Nytimes.com*, 2015. [Online]. Available: http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html

[27] T. Starner and S. Mann, "Augmented reality through wearable computing.," *Presence Teleoperators Virtual Environ.*, vol. 6, no. 4, p. 386, 1997.

[28] S. Mann and J. Fung, "EyeTap Devices for Augmented, Deliberately Diminished, or Otherwise Altered Visual Perception of Rigid Planar Patches of Real-World Scenes.," *Presence Teleoperators Virtual Environ.*, vol. 11, no. 2, pp. 158–175, 2002.

[29] S. Mann, "Fundamental issues in mediated reality, WearComp, and camera-based augmented reality," *Fundam. Wearable Comput. Augment. Reality, Lawrence Erlbaum Assoc. Inc*, pp. 295–328, 2001.

[30] S. Mann, "Steve Mann: My 'Augmented' Life," *IEEE Spectr.*, pp. 1–6, 2013.

[31] Cicso, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper," *Cisco Public*, 2016. .

[32] Cisco Systems 2017, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper," 2017.

[33] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A Survey on Mobile Edge Networks: Convergence of Computing, Caching and Communications," *IEEE Access*, 2017.

[34] P. Corcoran and S. K. Datta, "Mobile-Edge Computing and the Internet of Things for Consumers: Extending cloud computing and services to the edge of the network.," *IEEE Consum. Electron. Mag.*, 2016.

[35] P. Corcoran, "Mobile-Edge Computing and Internet of Things for Consumers: Part II: Energy efficiency, connectivity, and economic development," *IEEE Consum. Electron. Mag.*, 2017.

[36] F. Rumsey, "Binaural challenges: Spatial audio," *AES: Journal of the Audio Engineering Society*. 2014.

[37] A. McArthur, M. Sandler, and R. Stewart, "Distance in audio for VR: Constraints and opportunities," *ACM Int. Conf. Proceeding Ser.*, 2017.

[38] V. Algazi and R. Duda, "Headphone-based spatial sound," *IEEE Signal Process. Mag.*, 2011.

[39] J. A. Belloch, M. Ferrer, A. Gonzalez, F. J. Martinez-Zaldivar, and A. M. Vidal, "Headphone-based virtual spatialization of sound with a GPU accelerator," *AES J. Audio Eng. Soc.*, 2013.

[40] F. Rumsey, "Immersive audio: Objects, mixing, and rendering," *AES: Journal of the Audio Engineering Society*. 2016.

[41] P. Coleman, A. Franck, P. J. B. Jackson, R. J. Hughes, L. Remaggi, and F. Melchior, "Object-based reverberation for spatial audio," in *AES: Journal of the Audio Engineering Society*, 2017.

[42] M. Frank, F. Zotter, and A. Sontacchi, "Producing 3D Audio in Ambisonics," *Proc. 57th AES Int. Conf.*, 2015.

[43] R. Gupta, B. Lam, J. Hong, Z. Ong, W. Gan, S. H. Chong, and J. Feng, "3D audio AR/VR capture and reproduction setup for auralization of soundscapes," in *Proceedings of the 24th Intl. Congress on Sound and Vibration, ICSV24*, 2017.

[44] H. Kim, R. J. Hughes, L. Remaggi, P. J. B. Jackson, A. Hilton, T. J. Cox, and B. Shirley, "Acoustic room modelling using a spherical camera for reverberant spatial audio objects," in *142nd*

Audio Engineering Society Intl. Convention, AES 2017.

[45] T. Gholamalizadeh, H. Pourghaemi, A. Mhaish, and D. J. Duff, "Sonification of 3D Object Shape for Sensory Substitution : An Empirical Exploration," in *The Tenth Intl. Conference on Advances in Computer-Human Interactions (ACHI 2017)*, 2017.

[46] Timekeeper, "The promise of augmented reality," *Econ.*, 2017.

[47] R. Spolaor, Q. Q. Li, M. Monaro, M. Conti, L. Gamberini, and G. Sartori, "Biometric authentication methods on smartphones: A survey," *PsychNology J.*, 2016.

[48] A. De Luca, A. Hang, E. von Zezschwitz, and H. Hussmann, "I Feel Like I'm Taking Selfies All Day!," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, 2015.

[49] S. Karthikeyan, S. Feng, A. Rao, and N. Sadeh, "Smartphone fingerprint authentication versus pins: A usability study (cmu-cylab-14-012)," 2014.

[50] N. Zirjawi, Z. Kurtanović, and W. Maalej, "A survey about user requirements for biometric authentication on smartphones," in *2nd Intl. Workshop on Evolving Security and Privacy Requirements Engineering, ESPRE 2015 - Proceedings*, 2015.

[51] S. Thavalengal, P. Bigioi, and P. Corcoran, "Iris authentication in handheld devices - considerations for constraint-free acquisition," *IEEE Trans. Consum. Electron.*, vol. 61, no. 2, pp. 245–253, May 2015.

[52] S. Thavalengal, I. Andorko, A. Drimbarean, P. Bigioi, and P. Corcoran, "Proof-of-concept and evaluation of a dual function visible/NIR camera for iris authentication in smartphones," *IEEE Trans. Consum. Electron.*, vol. 61, no. 2, pp. 137–143, May 2015.

[53] A.-S. Ungureanu, S. Thavalengal, T. E. Cognard, C. Costache, and P. Corcoran, "Unconstrained palmprint as a smartphone biometric," *IEEE Trans. Consum. Electron.*, vol. 63, no. 3, pp. 334–342, Aug. 2017.

[54] P. Corcoran, "Beyond stream processing??? A distributed vision architecture for the Internet of Things," *2016 IEEE Int. Conf.*, 2016.

[55] S. Thavalengal, R. Vranceanu, R. G. Condorovici, and P. Corcoran, "Iris pattern obfuscation in digital images," in *IEEE Intl. Joint Conference on Biometrics*, 2014, pp. 1–8.

[56] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009, vol. 5672 LNCS, pp. 235–253.

[57] M. Ra, "P3 : Toward Privacy-Preserving Photo Sharing," *Nsdi*, pp. 515–528, 2013.

[58] L. Yuan, D. McNally, and A. Küpçü, "Privacy-preserving photo sharing based on a public key infrastructure," in *Proc SPIE 9599: Applications of Digital Image Processing XXXVIII*, 2015, p. 95991I–95991I.

[59] L. Yuan, P. Korshunov, and T. Ebrahimi, "Privacy-preserving photo sharing based on a secure JPEG," in *Proceedings - IEEE INFOCOM*, 2015, vol. 2015–Augus, pp. 185–190.

[60] J. P. Dunning, "Taming the blue beast: A survey of bluetooth based threats," *IEEE Secur. Priv.*, vol. 8, no. 2, pp. 20–27, 2010.

[61] K. Albrecht and L. McIntyre, "Protect Yourself from RFID: Fend off frightening tracking tech.," *IEEE Consumer Electronics Magazine*, vol. 4, no. 2. pp. 95–96, 2015.

[62] J. Hermans, R. Peeters, and B. Preneel, "Proper RFID privacy: Model and protocols," *IEEE Trans. Mob. Comput.*, vol. 13, no. 12, pp. 2888–2902, 2014.

[63] G. Arfaoui, S. Gambs, P. Lacharme, J.-F. Lalande, L. Roch, and J.-C. Paillès, "A Privacy-Preserving Contactless Transport Service for NFC Smartphones," *Fifth Int. Conf. Mob. Comput. Appl. Serv.*, vol. 130, pp. 282–285, 2013.

[64] P. Urien and S. Piramuthu, "Framework and authentication protocols for smartphone, NFC, and RFID in retail transactions," in *Proceedings of the 2013 IEEE 8th Intl. Conference on Intelligent Sensors, Sensor Networks and Information Processing: Sensing the Future, ISSNIP 2013*, 2013, vol. 1, pp. 77–82.

[65] H. Eun, H. Lee, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," *IEEE Trans. Consum. Electron.*, vol. 59, no. 1, pp. 153–160, 2013.

[66] M. Iqbal and S. Lim, "Privacy implications of automated GPS tracking and profiling," in *IEEE Technology and Society Magazine*, 2010, vol. 29, no. 2, pp. 39–46.

[67] M. Bierlaire, J. Chen, and J. Newman, "A probabilistic map matching method for smartphone GPS data," *Transp. Res. Part C Emerg. Technol.*, vol. 26, pp. 78–98, 2013.

[68] J. Chen and M. Bierlaire, "Probabilistic multimodal map-matching with rich smartphone data," *J. Intell. Transp. Syst.*, vol. 2450, no. September, p. 130116133115000, 2013.

[69] P. Corcoran, "Of Cameras and Clouds [Notes from the Editor]," *IEEE Consum. Electron. Mag.*, vol. 2, no. 3, pp. 3–5, Jul. 2013.

[70] A. Andrae and P. M. Corcoran, "Emerging Trends in Electricity Consumption for Consumer ICT," Jul. 2013.

[71] P. Corcoran, "I Am Game of Thrones [Notes from the Editor]," *IEEE Consum. Electron. Mag.*, vol. 4, no. 3, pp. 3–7, Jul. 2015.

[72] P. Corcoran, "The Internet of Things: Why now, and what? s next?," *Consum. Electron. Mag. IEEE*, 2016.

[73] P. Corcoran, "Consumer Electronics and the Internet of Things [Society News]," *IEEE Consum. Electron. Mag.*, vol. 3, no. 3, pp. 29–34, Jul. 2014.

[74] S. Grzonkowski, P. M. Corcoran, and T. Coughlin, "Security analysis of authentication protocols for next-generation mobile and CE cloud services," in *2011 IEEE Intl. Conference on Consumer Electronics -Berlin (ICCE-Berlin)*, 2011, pp. 83–87.

[75] P. Lucey, J. F. Cohn, T. Kanade, J. Saragih, Z. Ambadar, and I. Matthews, "The extended cohn-kanade dataset (ck+): A complete dataset for action unit and emotion-specified expression," in *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition-Workshops*, 2010, pp. 94–101.

[76] A. R. Rivera, J. R. Castillo, and O. Chae, "Local directional number pattern for face analysis: face and expression recognition.," *Image Process. IEEE Trans.*, vol. 22, no. 5, pp. 1740–52, May 2013.

[77] I. Bacivarov, P. M. Corcoran, and M. Ionita, "Smart cameras: 2D affine models for determining subject facial expressions," *Consum. Electron. IEEE Trans.*, vol. 56, no. 2, pp. 289–297, May 2010.

[78] Y. Tie and L. Guan, "A Deformable 3-D Facial Expression Model for Dynamic Human Emotional State Recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 1, pp. 142–157, Jan. 2013.

[79] I. Song, H. J. Kim, and P. B. Jeon, "Deep learning for real-time robust facial expression recognition on a smartphone," *Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron.*, pp. 564–567, 2014.

[80] R. Rana, M. Hume, J. Reilly, R. Jurdak, and J. Soar, "Opportunistic and Context-Aware Affect Sensing on Smartphones," *IEEE Pervasive Comput.*, vol. 15, no. 2, pp. 60–69, 2016.

[81] H.-Y. Wu, M. Rubinstein, E. Shih, J. Guttag, F. Durand, and W. Freeman, "Eulerian video magnification for revealing subtle changes in the world," *ACM Trans. Graph.*, vol. 31, no. 4, pp. 1–8, 2012.

[82] T. Partala and V. Surakka, "Pupil size variation as an indication of affective processing," *Int. J. Hum. Comput. Stud.*, vol. 59, no. 1, pp. 185–198, 2003.

[83] M. Soleymani, M. Pantic, and T. Pun, "Multimodal Emotion Recognition in Response to Videos," *IEEE Trans. Affect. Comput.*, vol. 3, no. 2, pp. 211–223, Apr. 2012.

[84] I. Bacivarov, M. Ionita, and P. Corcoran, "Statistical models of appearance for eye tracking and eye-blink detection and measurement," *Consum. Electron. IEEE Trans.*, vol. 54, no. 3, pp. 1312–1320, Aug. 2008.

[85] D. W. Hansen and Q. Ji, "In the eye of the beholder: a survey of models for eyes and gaze.," *Pattern Anal. Mach. Intell. IEEE Trans.*, vol. 32, no. 3, pp. 478–500, Mar. 2010.

[86] P. M. Corcoran, F. Nanu, S. Petrescu, and P. Bigioi, "Real-time eye gaze tracking for gaming design and consumer electronics systems," *Consum. Electron. IEEE Trans.*, vol. 58, no. 2, pp. 347–355, 2012.

[87] "Eye-gaze systems - an analysis of error sources and potential accuracy in consumer electronics use cases," *IEEE Int. Conf. Consum. Electron.*, 2016.

[88] J. R. Bellegarda, "Large-scale personal assistant technology deployment: The siri experience," in *Proceedings of the Annual Conference of the Intl. Speech Communication Association, INTERSPEECH*, 2013, pp. 2029–2033.

[89] S. Koolagudi and K. Rao, "Emotion recognition from speech: a review," *Int. J. speech Technol.*, 2012.

[90] V. Mayer-Schönberger and Y. Padova, "REGIME CHANGE? ENABLING BIG DATA THROUGH EUROPE'S NEW DATA PROTECTION REGULATION," *T H E C O L U M B I A Sci. Technol. LAW Rev.*, 2016.

[91] T. Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Iowa Law Rev.*, 2017.

[92] R. M. G. Sanz, "AN APPROACH TO A NEW AGREEMENT FOR EU/USA TRANSANTLANTIC PERSONAL DATA FLOW: AMERICAN TECHNOLOGY AND EUROPEAN LAW IN CONFLICT," in *4th Intl. Multidisciplinary Scientific Conference on Social Sciences and Arts SGEM 2017, Book 1*, 2017.

[93] M. Butterworth, "The ICO and artificial intelligence: The role of fairness in the GDPR framework," *Comput. Law Secur. Rev.*, 2018.

[94] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," *Comput. Law Secur. Rev.*, 2018.