

Privacy in the age of Mobile XR

1st Author Name, 2nd Author Name, ..., nth Author Name

Affiliation (s)

Location, Country

Contact Emails

Abstract

Surveillance capitalism¹ is a business based on the commoditization of customers' information, with the consequent impact on their privacy, and opening the door to large-scale social manipulation.² are some examples.

This has brought the weaponization of social media³, where invisible actors can harm the public interest using personal information, profiling and exposing groups and individuals, and manipulating the social narrative in sophisticated manners.

XR (mixed or extended reality) is a group of technologies including Virtual Reality, Augmented Reality and Telepresence, among others. These technologies rely on a growing number of sensors that allow for an extreme deepening of the existing surveillance.

This paper analyzes the potential social impact of XR, as well as proposing strategies aiming at safeguarding users' privacy.

Keywords

XR, Mixed reality, surveillance, privacy, biometrics, altered reality, mediated reality, virtual reality.

Introduction

Concerns of personal and social privacy are old as human history. Once a civilization adopts the concepts of 'inner' and 'outer,' "it becomes impossible to avoid the idea of privacy by whatever name it may be called"⁴, with Socrates and other Greek philosophers explicitly discussing privacy. The first recorded legal case related to privacy dated from 1361 when "the Justices of Peace Act in England provided for the arrest peeping toms and eavesdroppers"⁵.

Information technology has a defining impact on privacy, both in our understanding of what constitutes the private space and on the development of tools that drill on this space. In effect, with the introduction of the mechanical press, in 1891, a new discourse on privacy was built, with American lawyers like Samuel Warren and Louis Brandeis publishing the first article on "the right to be let alone"⁶.

In the 1960s Alan Westin wrote "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the

relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve" According to John Holvast "Since 1967, there has almost not been a publication on this subject in which this definition is not presented."

"The development of philosophical notions of inalienable rights of the individual was heavily influenced by the experience of many countries both during the Second World War and under post-war Central and Eastern European governments where (generally) manually operated filing systems tracked dissident citizens and members of minorities." ... "Two decades later, with the commercialization of large mainframe computers, the first laws to protect "personal data" about individuals were drafted, based upon an internationally agreed framework but with a local interpretation⁷."

By 1976 - 1979 the 3rd Party Doctrine was established in the US with the ruling over *Smith v Maryland*, stating that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties⁸."

The European Union (OECD in that time) passed the Data Protection Directive in 1980 with specific guidelines to protect the privacy of individuals within Europe. All its members enacted it by the end of the '90s. In 2012 the GDPR (General Data Protection Regulation) was commissioned and approved in 2016, and finally implemented in May 2018. The legal implications of the GDPR and its practical consequences are recent and yet to be seen in its full potential⁹. Technical analysts have already pinpointed some loopholes and big problems¹⁰.

American regulations, however, do not have a similar framework like GDPR, but the territorial range of GDPR can affect American companies, especially if those

companies have any presence in Europe. The international scope of the GDPR is still part of an extensive discussion¹¹.

Beyond the evolution of the legislation, the issue of privacy is not solved just by the application of a law. There are many other technical and practical factors that add complexity to the problem.

Online privacy breaches produce several problems for the individual¹², like inadvertent disclosure of personal information, damage of reputation, rumors, and gossip, cyberbullying, unwanted contact or harassment, political or social persecution, and fraud in many forms.

The social consequences of privacy breaches are also relevant, for example, the harsh repression during the Bahrain uprising crackdown¹³, or the controversial meddling in politics in many countries by Cambridge Analytica to mention some.

Digital privacy

*"If you are not paying for it, you're not the customer; you're the product being sold"*¹⁴ - Metafilter user "blue_beetle"

As previously stated, a big part of privacy problems with online business models is related to Surveillance Capitalism¹⁵, where private information is commoditized and used as the primary source of revenue for corporations.

Some companies have a tradition of compulsory data mining¹⁶ of personal information stored for further analysis, with key "always on" features by default, and complex privacy settings.

The commercialization of user information that shares their data has been expanded even to the social contacts of a user. This means that certain data of individuals that don't authorize their data to be shared has been accessed and used via friends or contacts. The case of Facebook selling this kind of information was exposed in the Cambridge Analytica scandal¹⁷.

From the user's perspective, uninformed decisions towards terms of service (ToS) make people accept whatever rules are presented enabling the use of a popular service¹⁸. The rules stated in some ToS would often be rejected by users that have the chance to customize their privacy. When people get more informed, their online footprint and their identifiable information are minimized. Public awareness of

privacy issues in different social networks is growing with time, and online behavior continues to shift¹⁹.

Even when some legislation like the GDPR protects information when linked to a person's ID, methods exist to de-anonymize social network information, rendering these regulations useless²⁰.

Several problems arise in the social area, derived from individual surveillance applied to big groups of people, or societies. Examples like political meddling²¹, activists or social actors profiling²², political prosecution²³, restrictions to free speech, blacklisting and exposure of vulnerable minorities²⁴ show the consequences of these practices on a social scale.

The problems produced by privacy breaches that exist in the modern information age have not been solved. Societies and governments are waking to the implications of the state of affairs. The expansion of information that can be gathered using advanced XR devices will add a new dimension for this issue with unimaginable consequences.

XR

XR is an umbrella category that includes technologies such as Virtual Reality (VR), Augmented Reality (AR) and others that exist in Milgram's "Reality-Virtual Reality continuum"²⁵. Originally the term "MR" (mixed reality) was used in place of XR. Industry and modern manufacturers, however, have favored the term "XR" where "X" stands for current or future technologies. The Khronos Group, a consortium of the largest companies operating on the field, is actively developing OpenXR²⁶, a standardized framework, and API, aiming at the interconnection and unification of the currently fragmented AR and VR ecosystems. According to Kronos, the API will continually grow to include new technological developments, like haptics or new devices.

There are three main groups of XR technologies with somewhat different characteristics, mobile AR, Augmented reality Headsets and Virtual Reality headsets. The trend is that the lines differentiating the media are blurring and mixing.

Mobile AR has quickly reached the mass consumer market, while head-mounted AR (ARHMD) exists only in experimental devices or developer kits (Microsoft HoloLens, Magic Leap, and others), and VR headsets are already mature and robust consumer grade products.

AR-enabled phones usually use Google's ARCore or Apple's ARKit. Both systems have a strong interaction with biometric data²⁷ and sensing or scanning real environments.

In ARHMD devices, the trend has been to integrate a comprehensive array of sensors, that include eye tracking, spatial awareness sensors like 3D scanners or speech recognition. Some problems with the current devices like issues with highly illuminated environments, narrow fields of view, relatively low graphical quality, and unreliable background occlusion and geometric coherence²⁸, don't allow for very accurate and meaningful user spatial interactions. Besides, given the reduced user base these devices have, there are not many applications²⁹. The tools are still considered experimental.

In the area of VR, the functionality has improved dramatically lately, and some new features are being developed by different manufacturers. Those include facial motion capture or real-time lip-sync for animating characters (oculus lip-sync SDK). Some add-ons can be attached to the VR headsets include electromyography³⁰ for facial tracking³¹, eye tracking and galvanic response³² to measure emotions, or 3D scanning devices like the leap motion.

In the mixed arena of consumer electronics, lots of devices now include physiological sensors and technologies akin to those used in the medical field. Those devices can connect to XR capable devices like mobile phones, and the information generated with those physiological sensors are also biometric signatures.

XR biometrics

Any measurement technique that allows the identification of a person is considered biometrics. This includes biological factors, behavioral patterns like writing and speech structure³³ among other makers.

The granularity of information available in XR devices allows identifying users through the combination of sensors. The information gathered can result in robust combined statistical analysis.

The adoption of biometrics in devices with fingerprint detection or face recognition has increased, thanks to their positive impact on usability (and, surprisingly, not due to other aspects like privacy and trust)³⁴.

Beyond the direct measurements for identification purposes, the biometric information is used to enhance user experiences. For example, the its depth camera used in iPhones "face ID" is also used to create AR video. Apple also shares abstract information of the face recognition systems with third-party developers making it available for them to capture, broadcast and store for further use³⁵.

Other problems with XR are the scanning of other potentially identifying informations (as many new XR devices have range imaging 3D cameras) as well as the scanning of private places, often without explicit consent. Examples like Roomba vacuum cleaner show the risks already present in consumer grade appliances³⁶.

Machine Learning algorithms also contribute to the mining of users' intimacy, inferring information about private spaces, objects, and other people around those devices. Experiments with the first commercial Google smart glass showed how it was possible to guess the location of users by their gazing at landmarks³⁷.

Manufacturers of new hardware and frameworks for XR include AI architectures and algorithms. That is the case of Qualcomm Snapdragon XR1 platform that provides for advanced vision processing like AR, Inertial Odometry, Audio Assistants and visual Artificial Intelligence³⁸. The platform allows on-device AI for object classification, pose prediction, natural language understanding, and speaker recognition.

The exposure of biometrics to third-party programmers is a relevant issue, and as biometric information cannot be reissued when exposed (like a password, or a stolen credit card), it represents a higher risk.

The corporate practices and ToS in VR, AR and other XR services, software, and devices are not usually transparent enough, and their information practices lack accountability³⁹.

Due to the technical complexity and the growing range of sensors, it is difficult to pinpoint which kind of data is vulnerable. Mixed techniques like VIO (visual inertial odometry)⁴⁰ allow to calculate with a high level of precision 6DOF, but those calculations are only possible through the mixture of different sensors like cameras and IMUS that work at the same time to drive a result. That example can explain the complexity that can arise when combining a multitude of sensors working at the same time to measure many other things, not foreseeable just by analyzing sensors individually. Some of the malicious attacks using multi-sensors and predictive approaches are for example the hacking of passwords techniques, (accelerometer side channel exploit), that allows predicting the password because of the motion of the phone while the user is entering the password⁴¹.

Many biometric signatures are vulnerable to side-channel timing attacks, so the idea of creating purely anonymous embodied information is challenging.

Even if the information is not read and archived by a provider of software or hardware, the act of broadcasting information to a virtual environment potentially opens the door to an automatic agent that's measuring the user's biometric signatures.

Some of the foreseeable externalities of XR technologies include behavioral profiling and prediction, private space and human relationship data mining. Emotional and psychological profiling and its commercial, legal or social exploitation.

A better future is possible

There are different strategies and regulations that can help to alleviate the risks introduced by XR, including new settings on the devices, new regulations, and informing and education of users. However, it is important to bear in mind that these are not enough and constant monitoring and introduction of new safeguards is necessary.

Regulations

The following is a list of settings that should be enforced in XR.

- The default settings for XR devices regarding privacy should be clear and easy to understand.
- The default settings should allow to “opt-in” instead of opting out for biometric sensing.
- Clarity of the purpose of biometric data to be collected.
- No punitive impact for the user when opting out from biometric data collection.
- In case the device needs biometric data, or 3d scanning to perform specific functions, the data should be processed locally when possible and avoid broadcasting personal data to be handled elsewhere.
- There is a need for accountability of the information gathered by a provider. (where the data goes and why).
- Vulnerable populations need special safe wards against the exposure of relevant information through XR: minorities, religious, cultural, sexual orientation.
- The recollection of data for further use should not be allowed. In the case that the recollected information would be used differently, a new consent from the individual should be required.
- Determination of the shared ownership of the data mined by XR devices, and the possibility to audit and delete such data by the users.
- The legal framework needs to be preemptive instead of reactive due to the permanent and not modifiable nature of biometric information (it can't be reissued once compromised)

Technical suggestions for manufacturers

- End to end encryption of data.
- Minimum storage for biometric data.

¹ Shoshana Zuboff, “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization,” *Journal of Information Technology* 30, no. 1 (March 1, 2015): 75–89, doi:10.1057/jit.2015.5.

² P. W. Singer and Emerson T. Brooking, *Likewar: The Weaponization of Social Media* (Boston: Eamon Dolan/Houghton Mifflin Harcourt, 2018).

³ Ibid.

- Limit the time for data to be stored.

Self-regulation strategies for the industry

- Creation of a standard like PEGI related to privacy.
- Industry association discussions.
- Best practice services and guidelines.
- Industry awards for privacy excellence.
- Privacy certification.
- Institutional boards or industrial association boards.

Education and desirable social behavior

- Inform of the consequences of privacy breaches by XR and biometrical devices
- Implications of the acceptance of invasive technologies according to the technology and use of it.
- Social condemnation of invasive corporate practices.
- Banning specific devices from private or spaces.
- Promoting and participating in Boycott against unethical corporate behavior.

Conclusions

XR is a new, rapidly growing field that threatens not only to translate but also worsen the social impacts of data-based capitalism, by integrating biometric and contextual information.

The granularity of the information produced by multi-sensory systems allows for the relatively easy profiling identification of the users, often granting access to intimate information.

There are, however, several strategies that users, companies, and governments can systematically apply to alleviate the social impact of these new technologies.

On top of this, regulations will play a defining role in the protection of privacy within XR. However, XR also deepens the impact of existing legal loopholes while introducing new vulnerabilities. Therefore, new regulatory frameworks need to be developed to tackle problems that will rise from this growing field.

Bibliography

⁴ Milton R. Konvitz, “Privacy and the Law: A Philosophical Prelude,” *Law and Contemporary Problems* 31, no. 2 (1966): 272–280.

⁵ J. Holvast, *The Future of Identity in the Information Society* (Boston: Springer, 2009).

⁶ Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy,” *Harvard Law Review*, 1890, 193–220.

- ⁷ Marek Rejman-Greene, "Privacy Issues in the Application of Biometrics: A European Perspective," in *Biometric Systems* (Springer, 2005), 335–359.
- ⁸ Orin S. Kerr, "The Case for the Third-Party Doctrine," *Mich. L. Rev.* 107 (2008): 561.
- ⁹ F. Moos, "The Troubling Reach of the GDPR Right to Data Portability," *E-Comm Law Policy* 18, no. 2 (2016): 9–10.
- ¹⁰ Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Seton Hall L. Rev.* 47 (2016): 995.
- ¹¹ Brendan Van Alsenoy, "Reconciling the (Extra) Territorial Reach of the GDPR with Public International Law," 2017.
- ¹² Bernhard Debatin et al., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication* 15, no. 1 (October 1, 2009): 83–108, doi:10.1111/j.1083-6101.2009.01494.x.
- ¹³ Singer and Brooking, *Likewar*.
- ¹⁴ "You're Not the Customer; You're the Product – Quote Investigator," accessed December 19, 2018, <https://quoteinvestigator.com/2017/07/16/product/>.
- ¹⁵ Zuboff, "Big Other."
- ¹⁶ Helen Kennedy, *Post, Mine, Repeat: Social Media Data Mining Becomes Ordinary* (Springer, 2016).
- ¹⁷ Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, March 17, 2018, sec. News, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
- ¹⁸ Thomas J. Maronick, "Do Consumers Read Terms of Service Agreements When Installing Software?—A Two-Study Empirical Analysis—," *International Journal of Business and Social Research* 4, no. 6 (2014): 137–145.
- ¹⁹ Mary Madden, "Privacy Management on Social Media Sites," *Pew Internet Report*, 2012, 1–20.
- ²⁰ Arvind Narayanan and Vitaly Shmatikov, "De-Anonymizing Social Networks," in *Security and Privacy, 2009 30th IEEE Symposium On* (IEEE, 2009), 173–187.
- ²¹ Carmen Reinhart and Kenneth Rogoff, "Regulation Should Be International," *Financial Times* 18 (2008).
- ²² Eytan Bakshy, Solomon Messing, and Lada A. Adamic, "Exposure to Ideologically Diverse News and Opinion on Facebook," *Science* 348, no. 6239 (2015): 1130–1132.
- ²³ Seva Gunitzky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," *Perspectives on Politics* 13, no. 1 (2015): 42–54.
- ²⁴ Kath Browne, "Snowball Sampling: Using Social Networks to Research Non-Heterosexual Women," *International Journal of Social Research Methodology* 8, no. 1 (2005): 47–60.
- ²⁵ Paul Milgram and Fumio Kishino, "A Taxonomy of Mixed Reality Visual Displays," *IEICE TRANSACTIONS on Information and Systems* 77, no. 12 (1994): 1321–1329.
- ²⁶ "OpenXR -," *The Khronos Group*, December 6, 2016, <https://www.khronos.org/openxr/>.
- ²⁷ Alexander De Luca et al., "I Feel like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (ACM, 2015), 1411–1414.
- ²⁸ D. W. F. Van Krevelen and Ronald Poelman, "A Survey of Augmented Reality Technologies, Applications and Limitations," *International Journal of Virtual Reality* 9, no. 2 (2010): 1.
- ²⁹ "Microsoft HoloLens Sales Figures Revealed – VRFocus," accessed December 11, 2018, <https://www.vrfocus.com/2018/05/microsoft-hololens-sales-figures-revealed/>.
- ³⁰ "Frequently Asked Questions," *Emteq*, accessed December 17, 2018, <https://emteq.net/faq/>.
- ³¹ "Home," *FOVE Eye Tracking Virtual Reality Headset*, accessed December 17, 2018, <https://www.getfove.com/>.
- ³² Doron Friedman, Kana Suji, and Mel Slater, "SuperDreamCity: An Immersive Virtual Reality Experience That Responds to Electrodermal Activity," in *International Conference on Affective Computing and Intelligent Interaction* (Springer, 2007), 570–581.
- ³³ H. Saevanee and P. Bhatarakosol, "User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device," in *2008 International Conference on Computer and Electrical Engineering*, 2008, 82–86, doi:10.1109/ICCEE.2008.157.
- ³⁴ De Luca et al., "I Feel like I'm Taking Selfies All Day!"
- ³⁵ <https://www.facebook.com/geoffreyfowler>, "Analysis | Apple Is Sharing Your Face with Apps. That's a New Privacy Worry," *Washington Post*, accessed December 19, 2018, <https://www.washingtonpost.com/news/the-switch/wp/2017/11/30/apple-is-sharing-your-face-with-apps-thats-a-new-privacy-worry/>.
- ³⁶ Maggie Astor, "Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared," *The New York Times*, January 20, 2018, sec. Technology, <https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html>.
- ³⁷ Hani Altwaijry, Mohammad Moghimi, and Serge Belongie, "Recognizing Locations with Google Glass: A Case Study," in *2014 IEEE Winter Conference on Applications of Computer Vision (WACV)* (IEEE, 2014), 167–174.
- ³⁸ "Qualcomm Reveals the World's First Dedicated XR Platform," *Qualcomm*, May 29, 2018, <https://www.qualcomm.com/news/releases/2018/05/29/qualcomm-reveals-worlds-first-dedicated-xr-platform>.
- ³⁹ Devon Adams et al., "Ethics Emerging: The Story of Privacy and Security Perceptions in Virtual Reality," 2018.
- ⁴⁰ Michael Bloesch et al., "Robust Visual Inertial Odometry Using a Direct EKF-Based Approach," in *Intelligent Robots and Systems (IROS), 2015 IEEE/RSJ International Conference On* (IEEE, 2015), 298–304.
- ⁴¹ Hwajeong Seo et al., "Open Sesame! Hacking the Password," in *International Workshop on Information Security Applications* (Springer, 2015), 215–226.