Facial Recognition Software Pros and Cons in the Privacy Age

Originally published at https://www.iflexion.com/blog/facial-recognition-software-pros-cons

Published: July 27, 2020 | By Martin Anderson

The meteoric rise of open-source facial recognition repositories and GPU-based machine learning has progressed faster than any legislative curbs or ethical and political guidelines could address it over the last five years. Estimated at $3.4 billion USD in 2019, the global market is currently forecast to rise to over $10 billion by 2027[1].

The key areas that have galvanized the sector leader in computer vision software development over the past five years are biometrics, security applications, marketing and attendance systems — all bolstered by recent advances in machine learning and the increasing use of lightweight mobile deep learning frameworks.

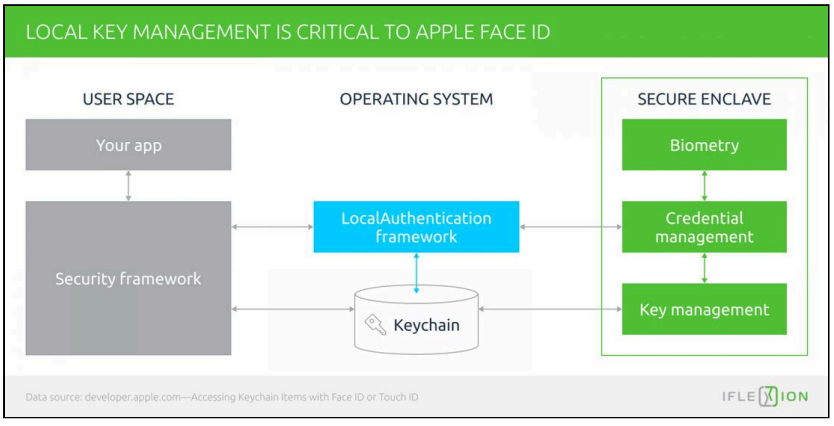
We'll examine some of these individual markets, but we'll also acknowledge that the facial recognition landscape is changing rapidly. The good news is that these changes are historically inevitable, and usually lead to a stable and more profitable sector with stricter legislation but fewer risk factors for new investors in the technology.

How Businesses Are Currently Using Facial Recognition Apps

The best-publicized uses of facial recognition software in commercially available products come from the companies that have invested most in such systems, each with a user base substantial enough to both feed and exploit massive amounts of incoming facial ID data.

Apple Face ID

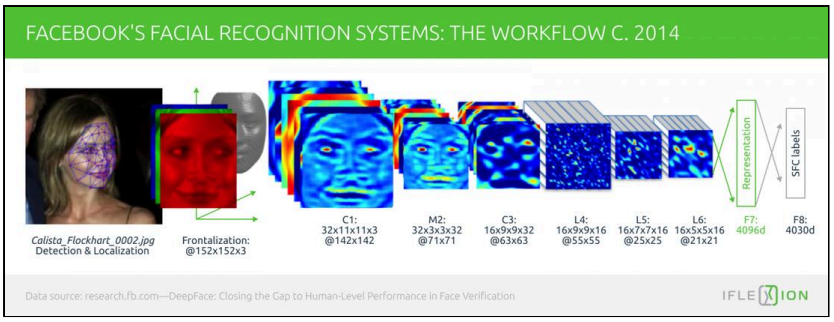
Apple's sophisticated deployment of face-based login for iOS uses several facets of a facial scan in order to verify the user, including 30,000 distinct facial data points and the use of infra-red imaging for 'liveness', a technique that is difficult to subvert[2]. However, Face ID has come under criticism for occasionally failing to individuate twins[3], for situations where it could not distinguish Chinese faces[4], and for periodic downtime[5].



In June 2020, Apple announced that it will extend Face ID's reach via a Web Authentication API, allowing users to log in to websites with their faces — a move generally welcomed by the tech community[6], considering that Apple has no corporate remit to commercialize user data.

Facebook

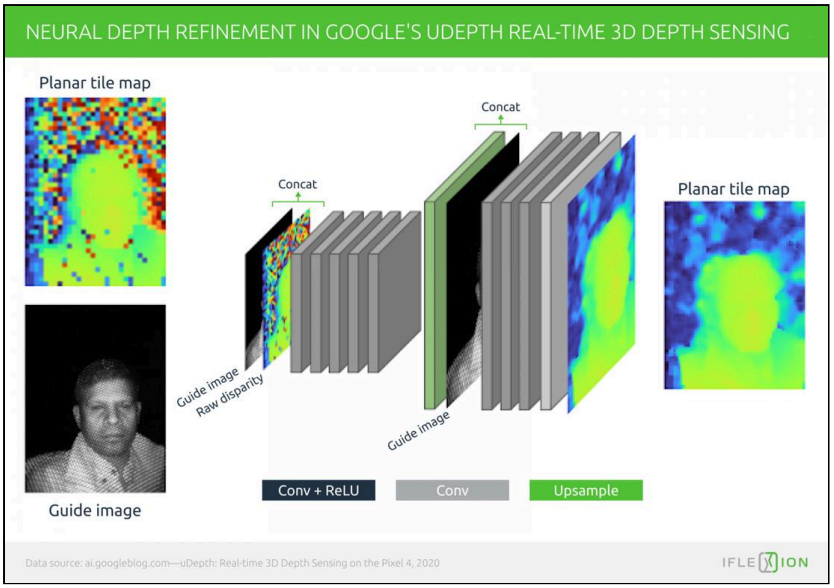
Facial recognition has been the cornerstone of Facebook's AI research over the last ten years. Since 2016, in the wake of the publication of its DeepFace neural net FR system[7], the social network has deployed it to identify users that are tagged in photo and video material uploaded by others.



In September of 2019, under pressure from lawsuits[8], privacy campaigners and the federal government[9], Facebook gave its users the ability to turn off a range of facial recognition settings for their accounts[10]. In January 2020, the company also agreed to pay $550 million USD to settle a lawsuit regarding privacy violations around facial recognition data in Illinois[11].

Google

Google operates one of the best-funded AI research initiatives in the world[12], with much of this effort devoted to the improvement of facial recognition architectures. The company has deployed its research for purposes of photo tagging (on Google Photos and for its search capabilities) and for Android-based logins, among other applications.



Google is one of the defendants in the State Of Illinois lawsuit[13], which maintains that — together with Microsoft, Facebook, and Amazon — the search engine giant has abused user-uploaded content in violation of state privacy laws. It's not a specious lawsuit, since a growing number of US states are fighting back against tech giants' *laissez-faire* usage of user content for facial recognition purposes[14].

In October of 2019, Google temporarily suspended facial recognition research for its Pixel 4 smartphone after it came to light that contracted researchers were targeting minority subjects from the student and homeless communities in order to re-balance the racial bias that besets FR systems[15]. Work has since resumed on the system[16].

Amazon

Amazon's Rekognition system was first leased to police authorities in 2017. Further deployments, including a controversial and aborted use by Orlando police in Florida in 2019[17], among other incidents, culminated in a grassroots protest from Amazon employees, who, together with numerous academic voices, successfully lobbied their bosses to limit the sale of facial recognition products to police, military and government services[18,19].

In June 2020, Amazon surprised the sector with a sweeping retraction of the sale of its facial recognition technology to police authorities, stating that it would end the one-year moratorium pending new legislation from the US Congress[20].

This is where Apple, Facebook, Google, and Amazon are with their facial recognition implementations right now

The Changing Face of Facial Recognition

There's significant evidence that the 'wild west' years of facial recognition are drawing to a close under pressure from privacy campaigners and from the politicians tasked with juggling the interests of the state with the will of voters.

Over the next five to ten years, increasing regulation is set to rationalize research and deployment of facial recognition technologies into a more stable state. New legislative boundaries are likely to cut away the early opportunists but leave behind a regulated industry that's ready to enter a more traditional business cycle of competition and conglomeration.

Besides the extent to which the advent of COVID-19 has altered the facial recognition landscape with intelligent video analytics, other political and social pressures have begun recently to bear down on its use, both in the private and public sector:

- In June 2020, IBM sent a letter to the United States House of Representatives, stating that it will no longer supply facial recognition or analysis software and urging a “national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies”[21].
- Public calls increased for a general moratorium on facial recognition technologies until suitable regulation is established[22], after the Washington Post revealed that the Federal Bureau of Investigation and Immigration and Customs Enforcement (ICE) transposed state driver’s license records into a facial recognition database without consent[23].
- In June 2020, Microsoft imposed a ban on the sale of facial recognition technologies pending clear and agreeable legislation[24].
- The trial rollout of a facial recognition scheme by the UK's Metropolitan Police together with controversies about the force's ad-hoc use of facial recognition[25], has increased calls for more oversight mechanisms[26].
- At the same time that prominent privacy regulators warn that AI-based facial recognition could become illegal in the European Union[27], pan-European police forces are pushing for an EU-wide facial recognition database[28].

The current lack of consensus is creating a turbulent and volatile landscape for business investors in facial recognition. When even a notable company such as IBM abandons it as a PR liability, under pressure from shareholders responding to public sentiment[29], we can assume that automated facial ID technologies have arrived at a critical juncture.

Regulation as an Enabler for Business Facial Recognition Systems

In fact, increased regulation and growing public skepticism is more likely a sign that the new technology is beginning a long-term relationship with the society, negotiating the terms of its future successes. Some of the most revolutionary technological advances, such as the printing press and genetic engineering, proliferated their way into regulation and rationalization, usually under protest from their proponents.

When crowdsourced data and open-source technologies are perceived as a global challenge to governments around the world[30], the result is, historically, assimilation and regulation rather than annihilation or prohibition.

This regulated environment is the inevitable future of facial recognition for business. Deployments are not an issue: world-leading open-source libraries, funded or co-funded by the biggest tech entities on the planet, are a massive enabler for facial recognition project development. The key to a successful project, rather, is governance and due diligence regarding the project's scope and legal exposure.

A regulated environment is the inevitable future of facial recognition for business.

Future-Proofing Your Facial Recognition Deployment

Though legislation around facial recognition technologies is in flux around the world as well as within the individual states of the US[31], a rigorous approach to data governance and a thorough acquaintance with local and national laws is fundamental to the longevity of a business facial recognition deployment.

1: Be Aware of Existing and Pending Regulations

Consult your national and, where applicable, state's legislature around privacy and data governance where it relates to facial recognition technologies. Stay aware of pending bills and amendments that may change the regulations at some future date.

Research current case studies of facial recognition deployments in the private and the public sector, and acquaint yourself with clauses in recent legislation which facilitate implementations. These might include projects in the interests of national security, or where the use of facial recognition has been officially acknowledged as non-challengeable, such as in workplaces where facial recognition is included in the limited right-to-privacy of employees; prisons and other state institutions; educational environments; and experimental scenarios where the subjects have specifically opted in to facial recognition, and where such exceptions are permitted by local and national laws.

2: Build Data Governance Mechanisms into Facial Recognition Projects from the Outset

Even where current regulations may not require it, your facial recognition project should have accessible, human-readable policies around data retention, which in turn should fall in line with at least the minimum requirements of applicable law for your area.

Provide mechanisms where users can be apprised of the facial recognition data they have generated, and means by which the users can delete their data and/or opt out of the facial recognition scheme. Even if there is no current legal necessity to provide this functionality, it may be required in the future and will be far easier and cheaper to implement (and hide) at the start rather than retrofit if it should be needed later.

3: Maintain Detailed Long-Term Logs

Implement a comprehensive and secure logging system in accordance with any prevailing laws that may specify policies around scope, granularity and retention of logs for the use and passage of facial recognition data.

4: Define and Publish Clear Information Around Sharing of Facial Recognition Data

A transparent approach to the journey of users' facial recognition information is essential. With the exception of *sub judice* requests from authorities, or where requirements for data retention may have expired, it should remain possible to deliver a complete account of where and when facial recognition data has been shared with parties included in the terms of an opt-in, or more generally under prevailing local and national laws.

5: Check for Bias, Even If You Need Bias

Most goal-oriented facial recognition projects are in search of a relevant subset of surveilled subjects, whether the aim is marketing (most likely buyers), security (most likely offenders), or any other sector.

However, the National Institute of Standards and Technology (NIST) has identified 'empirical evidence' of racial and gender bias among some of the most popular algorithms and datasets[32], while individuals of color have been falsely identified by facial recognition systems used by authorities[33].

Where facial recognition is a subset of object recognition/segmentation, the PR nightmares can multiply: Google was put in an uncomfortable position after its own facial recognition software defined two ethnic subjects as 'gorillas'[34].

It's inevitable that the goals of a facial recognition program will drill down to 'median' subjects, who may or may not have any particular characteristics in common among themselves. But it's essential to ensure that your tools and dataset development techniques are engineered to be impartial. Don't aim for results that you're already expecting and ensure any eventual distilled data were developed neutrally, being ready to demonstrate it later if necessary.

With biased facial recognition technology, PR nightmares can easily multiply.

Conclusion

If identity has become the new currency, then developing a facial recognition system will in the next ten years require the same diligence and adherence to regulation as creating a banking system, where handling the money itself is a relatively trivial logistic, but overseeing its safe and legal passage and usage is the central challenge.

The current wave of public resistance to unregulated facial recognition has already thinned down the lazy opportunists — the business models that failed to see that ad-hoc facial recognition deployment would inevitably hit a firewall of public objection, leaving the sector to evolve into a regulated and useful industry with acceptable checks and balances and appropriate terms of entry.

It's this serious mindset that will distinguish the most successful uses of facial recognition in the public and private sector in the years to come.