FACIAL RECOGNITION TECHNOLOGY

"I never forget a face, but in your case I'll be glad to make an exception." *Groucho Marx*. As Groucho Marx's classic line reminds us, we humans do have the option to occasionally forget faces whenever we really want to. This can be a good thing, but for those in the burgeoning biometrics field of computer-assisted facial recognition technology, the goal is never to forget a face – without exception.

Matching a set of eyes, ears, nose and mouth to a single individual through facial recognition (FR) has become, to put it simply, huge. The field's late 20th Century beginnings may have been clumsy at first, but researchers knew they had something big on their hands. Now, in 2013, the technology is far from full-grown, but like an adolescent, it's maturing fast. How reliable has FR become? At this point, computer software can quickly and accurately identify a person with only a one-in-a-thousand chance of error, and that's just from a "glance" at one decent photo. We're now staring into a fast-approaching future that will, without a doubt, see this ID success rate skyrocket.

The gaming revolution will be digitized

On a global level, how interested are we really in FR technology? Google the term "facial recognition" and see for yourself. Those millions of hits give the answer: "extremely interested." What's more, notice the level of sheer controversy we're already facing. You'll see it on the first page of results: privacy issues, intellectual property concerns, fair business practices; questions like these are already swarming around the technology, which can only mean one thing: FR is not going away. As we saw with digital music in the '80s, CGI-filmmaking in the '90s, and file-sharing over the last decade, heavy controversy means revolution, and that's exactly what facial recognition is.

Whichever way these legal and ethical quandaries resolve themselves over time, public and private organizations of all stripes are grasping just how important it is to pay attention. Staying on the right side of FR technology will be crucial to ensuring functional and financial success, and sure enough, everyone from Smart TV manufacturers to top-level national security organizations worldwide are now buying in big. Naturally, you'd expect the gaming industry to run near the front of that pack; you'd expect correctly.

In fact, Canada's trendsetting Ontario Lottery and Gaming Corporation (OLG) was all over the movement as long as two years ago, when the agency implemented facial recognition systems in all 27 of the province's gambling venues. Now, the Ontario slots have "eyes" that can recognize any problem gambler who has previously (and voluntarily) submitted his or her photo to a casino database. If this person sits down at a machine, security is alerted and the gambler is "eighty-sixed," saving them from themselves – and saving the casino from the potential lawsuit that can result from gamblers blowing self-destructively through their nest eggs. So far, OLG's land-based program has been a success. It also reveals something about what FR technology can promise for the online gaming community.

Let the right one in

Online customers, if they're going to remain customers, need deep assurances that their identities are safe. That's a real and growing concern, because let's face it, the prevailing vibe these days is that being "safe" online is like being "safe" on a raft in shark-infested waters. Lately, popular news sites have been rife with chilling headlines about password insecurity, hackers on the rampage and grand-scale data heists pulled off everywhere, even on vast corporate and government entities that once seemed so invulnerable. In addition to teams of cyber-security experts, the biggest companies are now employing full-time legal and PR staff just to stop the bleeding in case customer data is, or has already been, compromised.

The point is this: if Amazon needs its customers to know that its information is safely locked down, you can bet that an online casino needs its customers to know that their data is watched-over 24/7 by a digital legion of armed guards. Investing in facial recognition software sure looks like a good move toward building that kind of cyber-security force in these cyber-uncertain times.

The move is already happening. Ever since they first arrived on the scene, online casinos and sportsbetting sites have used state-of-the-art methods of data encryption to protect customer credit card and bank account information. But as risks of fraud and identity theft have begun to loom larger on the online landscape, it's become apparent that a better mousetrap is in order.

Facing the future

Enter Facebanx. The UK-based company may be relatively small, but its recently developed facial recognition software is quickly gaining traction where secure log-ins are concerned. Instead of the traditional alphanumeric passwords that can be hacked (or, too often, simply found on "hidden" sticky-notes under the keyboard), Facebanx is going down the far more personal route. As part of a one-time set-up procedure for new accounts, system users are recorded live via webcam or other video-capable smart devices. It's like an online dating site, except that you're simply being matched with yourself, because that little computer-analyzed movie then becomes a kind of dynamic user ID card. For every subsequent log-in, the software checks a fresh image capture against the video to ensure that the person sitting there is really you. Online UK casinos Grosvenor and Ladbrokes are already looking into it, along with other high-profile Internet entities who require the highest level of protection available for customer data and credit card/bank account transactions.

And Facebanx isn't the only game in town; with online gambling now legal in Delaware, New Jersey and Nevada (and more states soon to come), fraud-protection specialists at Washington DC-based LaserLock Technologies are marketing their own next-generation solution to online casinos stateside. With its VerifyMe software platform, LaserLock actually combines FR technology with geolocation tracking to make doubly certain of users' identities before granting access.

Preparing for the expected

"What if I just hold a picture of a registered player up to the camera," you ask? Good question, and you're not the first to pose it. You might try looking again to Google for the answer – not the actual search engine in this case, but the company itself. It seems the uber-tech giant has just filed for a patent for a newly developed FR method that would "keep it real" by asking a bit more from system users. Rather than just smiling for a single snapshot, Google's protocol would require you to do something random and more elaborate like, say, scrunch up your nose and then wink. Or raise one eyebrow and smirk. In other words, something that a fraudulent, held-up photo just couldn't do, at least not easily or quickly enough to fool the software.

It's impressive stuff, no doubt. But is all this biometric layering and smirk/wink/nod detection getting a bit too complicated? Will serious users really be willing to jump though these strange new hoops just for the sake of a little additional peace of mind? Only time will tell, but for now, it's hard to imagine that they wouldn't. True, the public discussion of how to preserve online privacy is getting loud. It's also true that customers are now more aware and more edgy than ever about how much of themselves they're comfortable distributing online. That's why it becomes crucial to consider the stakes here. Yes, FR technology may well discourage users from more frivolous online ventures, such as installing hip new social network apps of the future. But comparing this to the high-security arena of bank accounts and online gaming is a matter of apples and oranges. When it comes to feeling secure that some cyber-thug isn't playing the slots on your hard-earned dime, suddenly Google's grins and winks don't seem like so much to ask.

Speaking of Google, there's some interesting, gaming-related irony to the sleek, Internet-connected Glass headwear it has just developed. Are these cyborg-like devices part of the facial recognition revolution? Absolutely. Proposed third-party FR apps for Glass are already in the works, despite Google's banning of them for now. Will Glass be allowed in casinos? Never, for the same reason that you can't sit down at the table with a video camera or an iPad. If facial recognition technology and Internet connectivity are going to be used in a land-based casino, naturally they're going to be the exclusive privilege of the house. After all, the house always has the edge.

Rob Gallo is Chief Executive Officer of Peak Gaming Group and can be reached at: robg@peakgaminggroup.com.