

# BEHIND YOUR BACK, YOUR CELL PHONE IS DESTROYING YOUR LIFE

Wed, 03 Aug 2022 12:26:57, newstips66, [post\_tag: behind-your-back, category: brotopia, category: community-service-programs, category: elon-musk, category: energy-dept-slush-fund, category: facebook-meta, category: google-alphabet, category: hired-assassins, category: lithium-batteries, category: netflix, category: news-manipulation, category: silicon\_valley\_death, category: sony\_pictures, category: stanford\_univ\_bribes, category: tesla\_motors\_lies\_and\_defects, category: web-spying, category: worldnews, post\_tag: your-cell-phone-is-destroying-your-life]

## Your Phone Is Killing You And Destroying Your Life

By Donna Lawson

Did you know that the electronics in your phone, AND, 99% of the 'Apps' on your phone are tracking you, spying on you, tricking you, and reporting to others when you:

- Get an abortion
- Have sex
- Get pregnant
- Don't go to work
- Enter, or leave, any building
- Get into, or out of, your car
- Have a sex worker take Uber, Lyft or any taxi or ride service to where you are
- Receive money
- Buy anything
- Are depressed
- Breath heavy
- Are located at any location on Earth
- Move from any location on Earth to another location
- Take anything out of your wallet with a chip in it
- Vote
- Express a political opinion
- Use a dating site (Axiom and Equifax make psych profiles on you from your date data)
- Use any 'gay' code words
- Use any 'political' code words
- Speak, or listen, to anyone within 20 feet
- And thousands of other invasions of privacy...

It does these things even if you pushed the button to 'turn it off'. Most phones don't actually turn off when you think they are off because 'spies-gotta-spy'.

COVID is doing a great job of killing off all of the idiot people who grab the door-knob, bare-handed, at the post office, the Starbucks and the grocery store. COVID waits on public surfaces to kill the sheep of society.

Silicon Valley is doing a great job of killing off all the lives of the rest of the sheep who are too dumb to take the battery out of their phone. The people that walk around with a phone, or tablet, always powered on are committing digital suicide. If you buy a phone that you can't take the battery out of, you are just an idiot.

You may not want to face the truth but I can show you thousands of court records, Congressional investigations and university studies proving that every single assertion in this report is true.

Everybody in Congress knows this is all true but they do nothing because Silicon Valley is bribing almost every single one of them to do nothing. Silicon Valley's largest source of income is your privacy! Silicon Valley will do anything to keep you from knowing how deadly your cell phone is to the quality of your life.

A search takes mere seconds. You upload a photo of a face, check a box agreeing to the terms of service and then get a grid of photos of faces deemed similar, with links to where they appear on the internet. The New York Times used PimEyes on the faces of a dozen Times journalists, with their consent, to test its powers.

PimEyes found photos of every person, some that the journalists had never seen before, even when they were wearing sunglasses or a mask, or their face was turned away from the camera, in the image used to conduct the search.

PimEyes found one reporter dancing at an art museum event a decade ago, and crying after being proposed to, a photo that she didn't particularly like but that the photographer had decided to use to advertise his business on Yelp. A tech reporter's younger self was spotted in an awkward crush of fans at the Coachella music festival in 2011. A foreign correspondent appeared in countless wedding photos, evidently the life of every party, and in the blurry background of a photo taken of someone else at a Greek airport in 2019. A journalist's past life in a rock band was unearthed, as was another's preferred summer camp getaway.

Unlike [Clearview AI](#), a similar facial recognition tool available only to law enforcement, PimEyes does not include results from social media sites. The sometimes surprising images that PimEyes surfaced came instead from news articles, wedding photography pages, review sites, blogs and pornography sites. Most of the matches for the dozen journalists' faces were correct. For the women, the incorrect photos often came from pornography sites, which was unsettling in the suggestion that it *could* be them. (To be clear, it was not them.)

A tech executive who asked not to be identified said he used PimEyes fairly regularly, primarily to identify people who harass him on Twitter and use their real photos on their accounts but not their real names. Another PimEyes user who asked to stay anonymous said he used the tool to find the real identities of actresses from pornographic films, and to search for explicit photos of his Facebook friends.

The new owner of PimEyes is Giorgi Gobronidze, a 34-year-old academic who says his interest in advanced technology was sparked by Russian cyberattacks on his home country, Georgia.

## ADVERTISEMENT

Mr. Gobronidze said he believed that PimEyes could be a tool for good, helping people keep tabs on their online reputation. The journalist who disliked the photo that a photographer was using, for example, could now ask him to take it off his Yelp page.

PimEyes users are supposed to search only for their own faces or for the faces of people who have consented, Mr. Gobronidze said. But he said he was relying on people to act "ethically," offering little protection against the technology's erosion of the long-held ability to stay anonymous in a crowd. PimEyes has no controls in place to prevent users from searching for a face that is not their own, and suggests a user pay a hefty fee to keep damaging photos from an ill-considered night from following him or her forever.

"It's stalkerware by design no matter what they say," said Ella Jakubowska, a policy adviser at European Digital Rights, a privacy advocacy group.

## Under new management

Mr. Gobronidze grew up in the shadow of military conflict. His kindergarten was bombed during the civil war that ensued after Georgia declared independence from the Soviet Union in 1991. The country was effectively cut off from the world in 2008 when Russia invaded and the internet went down. The experiences inspired him to study the role of technological dominance in national security.

After stints working as a lawyer and serving in the Georgian Army, Mr. Gobronidze got a master's degree in international relations. He began his career as a professor in 2014, eventually landing at European University in Tbilisi, Georgia, where he still teaches.

In 2017, Mr. Gobronidze was in an exchange program, lecturing at a university in Poland, when one of his students introduced him, he said, to two “hacker” types — Lucasz Kowalczyk and Denis Tatina — who were working on a facial search engine. They were “brilliant masterminds,” he said, but “absolute introverts” who were not interested in public attention.

They agreed to speak with him about their creation, which eventually became [PimEyes](#), for his academic research, Mr. Gobronidze said. He said they had explained how their search engine used neural net technology to map the features of a face, in order to match it to faces with similar measurements, and that the program was able to learn over time how to best determine a match.

“I felt like a person from the Stone Age when I first met them,” Mr. Gobronidze said. “Like I was listening to science fiction.”

He kept in touch with the founders, he said, and watched as PimEyes began getting more and more attention in the media, [mostly](#) of the [scathing variety](#). In 2020, PimEyes claimed to have a new owner, who wished to stay anonymous, and the corporate headquarters were moved from Poland to Seychelles, a popular African offshore tax haven.

Mr. Gobronidze said he “heard” sometime last year that this new owner of the site wanted to sell it. So he quickly set about gathering funds to make an offer, selling a seaside villa he had inherited from his grandparents and borrowing a large sum from his younger brother, Shalva Gobronidze, a software engineer at a bank. The professor would not reveal how much he had paid.

“It wasn’t as big an amount as someone might expect,” Mr. Gobronidze said.

In December, Mr. Gobronidze created a corporation, EMEARobotics, to acquire PimEyes and registered it in Dubai because of the United Arab Emirates’ low tax rate. He said he had retained most of the site’s small tech and support team, and hired a consulting firm in Belize to handle inquiries and regulatory questions.

Mr. Gobronidze has rented office space for PimEyes in a tower in downtown Tbilisi. It is still being renovated, light fixtures hanging loose from the ceiling.

Tatia Dolidze, a colleague of Mr. Gobronidze’s at European University, described him as “curious” and “stubborn,” and said she had been surprised when he told her that he was buying a face search engine.

“It was difficult to imagine Giorgi as a businessman,” Ms. Dolidze said by email.

Now he is a businessman who owns a company steeped in controversy, primarily around whether we have any special right of control over images of us that we never expected to be found this way. Mr. Gobronidze said facial recognition technology would be used to control people if governments and big companies had the only access to it.

And he is imagining a world where facial recognition is accessible to anyone.

## ‘Essentially extortion’

A few months back, Cher Scarlett, a computer engineer, tried out PimEyes for the first time and was confronted with a chapter of her life that she had tried hard to forget.

In 2005, when Ms. Scarlett was 19 and broke, she considered working in pornography. She traveled to New York City for an audition that was so humiliating and abusive that she abandoned the idea.

PimEyes unearthed the decades-old trauma, with links to where exactly the explicit photos could be found on the web. They were sprinkled in among more recent portraits of Ms. Scarlett, who works on labor rights and has been the subject of media coverage for a [high-profile](#) worker [revolt](#) she led at [Apple](#).

“I had no idea up until that point that those images were on the internet,” she said.

Worried about how people would react to the images, Ms. Scarlett immediately began looking into how to get them removed, an experience she described in a [Medium post](#) and to [CNN](#). When she clicked on one of the explicit photos on PimEyes, a menu popped up offering a link to the image, a link to the website where it appeared and an option to “exclude from public results” on PimEyes.

But exclusion, Ms. Scarlett quickly discovered, was available only to subscribers who paid for “PROtect plans,” which cost from \$89.99 to \$299.99 per month. “It’s essentially extortion,” said Ms. Scarlett, who eventually signed up for the most expensive plan.

Mr. Gobronidze disagreed with that characterization. He pointed to [a free tool](#) for deleting results from the PimEyes index that is not prominently advertised on the site. He also provided a receipt showing that PimEyes had refunded Ms. Scarlett for the \$299.99 plan last month.

PimEyes has tens of thousands of subscribers, Mr. Gobronidze said, with most visitors to the site coming from the United States and Europe. It makes the bulk of its money from subscribers to its PROtect service, which includes help from PimEyes support staff in getting photos taken down from external sites.

PimEyes has a free [“opt-out”](#) as well, for people to have data about themselves removed from the site, including the search images of their faces. To opt out, Ms. Scarlett provided a photo of her teenage self and a scan of her government-issued identification. At the beginning of April, she received a confirmation that her opt-out request had been accepted.

“Your potential results containing your face are removed from our system,” the email from PimEyes said.

But when The Times ran a PimEyes search of Ms. Scarlett’s face with her permission a month later, there were more than 100 results, including the explicit ones.

Mr. Gobronidze said that this was a “sad story” and that opting out didn’t block a person’s face from being searched. Instead, it blocks from PimEyes’s search results any photos of faces “with a high similarity level” at the time of the opt-out, meaning people need to regularly opt out, with multiple photos of themselves, if they hope to stay out of a PimEyes search.

Mr. Gobronidze said explicit photos were particularly tricky, comparing their tendency to proliferate online to the mythical beast Hydra.

“Cut one head and two others appear,” he said.

Mr. Gobronidze said he wanted “ethical usage” of PimEyes, meaning that people search only for their own faces and not those of strangers.

But PimEyes does little to enforce this goal, beyond a box that a searcher must click asserting that the face being uploaded is his or her own. Helen Nissenbaum, a Cornell University professor who studies privacy, called this “absurd,” unless the site had a searcher provide government identification, as Ms. Scarlett had to when she opted out.

“If it’s a useful thing to do, to see where our own faces are, we have to imagine that a company offering only that service is going to be transparent and audited,” Ms. Nissenbaum said.

PimEyes does no such audits, though Mr. Gobronidze said the site would bar a user with search activity “beyond anything logical,” describing one with more than 1,000 searches in a day as an example. He is relying on users to do what’s right and mentioned that anyone who searched someone else’s face without permission would be breaking European privacy law.

“It should be the responsibility of the person using it,” he said. “We’re just a tool provider.”

Ms. Scarlett said she had never thought she would talk publicly about what happened to her when she was 19, but felt she had to after she realized that the images were out there.

“It would have been used against me,” she said. “I’m glad I’m the person who found them, but to me, that’s more about luck than PimEyes working as intended. It shouldn’t exist at all.”

## Exceptions to the rule

Despite saying PimEyes should be used only for self-searches, Mr. Gobronidze is open to other uses as long as they are “ethical.” He said he approved of investigative journalists and the role PimEyes played in [identifying Americans](#) who stormed the U.S. Capitol on Jan. 6, 2021.

The Times allows its journalists to use face recognition search engines for reporting but has internal rules about the practice. “Each request to use a facial recognition tool for reporting purposes requires prior review and approval by a senior member of the masthead and our legal department to ensure the usage adheres to our standards and applicable law,” said a Times spokeswoman, Danielle Rhoades Ha.

There are users Mr. Gobronidze doesn’t want. He [recently](#) blocked people in Russia from the site, in solidarity with Ukraine. He mentioned that PimEyes was willing, [like Clearview AI](#), to

offer its service for free to Ukrainian organizations or the Red Cross, if it could help in the search for missing persons.

The better-known Clearview AI has faced serious headwinds in Europe and around the world. Privacy regulators in Canada, Australia and parts of Europe have declared Clearview's database of 20 billion face images illegal and ordered Clearview to delete their citizens' photos. [Italy](#) and [Britain](#) issued multimillion-dollar fines.

A German data protection agency announced an investigation into PimEyes [last year](#) for possible violations of Europe's privacy law, the [General Data Protection Regulation](#), which includes strict rules around the use of biometric data. That investigation is continuing.

Mr. Gobronidze said he had not heard from any German authorities. "I am eager to answer all of the questions they might have," he said.

He is not concerned about privacy regulators, he said, because PimEyes operates differently. He described it as almost being like a digital card catalog, saying the company does not store photos or individual face templates but rather URLs for individual images associated with the facial features they contain. It's all public, he said, and PimEyes instructs users to search only for their own faces. Whether that architectural difference matters to regulators is yet to be determined.

Sheelagh McNeill contributed research.

The post [A Face Search Engine Anyone Can Use Is Alarminglly Accurate](#) appeared first on [New York Times](#).