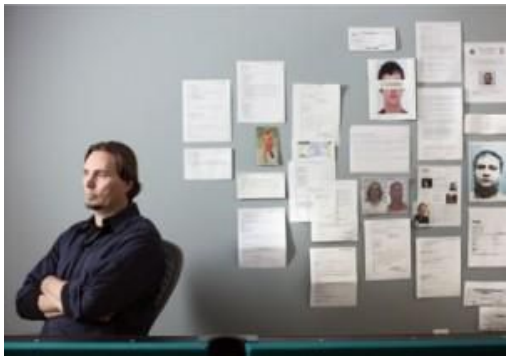
Facebook's Top Cop: Joe Sullivan

Kashmir Hill Forbes Staff
Welcome to The Not-So Private Parts where technology & privacy collide

This story appears in the March 12, 2012 issue of Forbes magazine.

If Facebook were a country, it would be the third largest in the world and Joe Sullivan would be head of Homeland Security.



Facebook chief of security Joe Sullivan, sitting in front of a display of the bad guys his team has taken down (Photo Credit:Timothy Archibald)

His actual title is chief security officer. The “terrorists” he’s up against include the “Koobface gang,” a quintet of Russians who unleashed a worm that turned - Facebookers’ computers into enslaved bots; the spammers who flooded the site with violent and pornographic images in December; scammers who trick Facebook users into clicking links and filling out surveys for the swindlers’ profit; pedophiles using the site to make contact with minors; and scrapers who inappropriately raid Facebook for users’ valuable personal information. These scoundrels include those who use malicious apps, hackers and an amateur porn - purveyor who matches profile pages to private nudie photos submitted by vengeful exes—making it easy to contact, harass and “poke” the unwitting and involuntary porn stars.

The dirt Facebook holds on its users makes it as attractive to cops as to criminals. Among Sullivan's responsibilities are daily decisions about how much user information to give to law enforcement when it comes calling. And, as a digital nation's DHS, Sullivan and his team actively police the site for user data worth volunteering to the authorities. Still, he says, "we err on the side of not sharing and have picked quite a few fights over the years."

Users may have constitutional rights against unreasonable searches by the state, but the only Facebook Constitution is the company's dense terms of service agreement. It focuses on prohibitions for users, such as bullying, creating fake accounts or uploading images of violence or nudity, as well as Facebook's rights to intellectual property uploaded to the site. It doesn't spell out when Facebook may dive into data for policing purposes or hand it over to the authorities.

Should Facebook give users a Miranda warning before they sign up—that anything they post and do on the site can and will be used against them? The company gives law enforcement "basic subscriber information" on requests accompanied by subpoenas: a user's name, e-mail address and IP address (which reveals approximate location). Sullivan insists that everything else—photos, status updates, private messages, friend lists, group memberships, pokes and all the rest—requires a warrant.

Sullivan, 43, usually wears the "Mark Zuckerberg uniform" at the office: gray hoodie, sneakers, jeans. With longish light-brown hair and gray-speckled goatee, he looks more like a bouncer at a country music bar than an ex-federal prosecutor, let alone the guy responsible for safeguarding and investigating Facebook's 845 million users.

Most of his security team is based at headquarters in Menlo Park, Calif. and sits at clusters of desks close enough to take dead aim at one another with Nerf darts. Broken roughly into five parts, the team has 10 people review new features being launched, 8 monitor the site for bugs and privacy flaws, 25 handle requests for user information from law enforcement, and a few build criminal and civil cases against those who misbehave on the network; the rest are handling security situations as they arise and acting as digital bodyguards protecting Facebook

staffers ("We have someone trying to hack an employee's account every day," says Sullivan). If you include the physical security guards who patrol Facebook headquarters, Sullivan's team numbers 70 people.

It's a big kingdom to police, populated with mundane and highly personal information about its subjects. Its value, shaping up to be $100 billion when the company goes public later this year, depends on keeping the populace happy and safe—from overprobing law officials, as well as from predators.

THE OLDEST OF SEVEN CHILDREN, Sullivan grew up in Cambridge, Mass. He describes his father as a painter and sculptor, and his mother as a schoolteacher who wrote mystery stories about a nun who was a private eye. "So I rebelled and went to law school," he says. (A Google search revealed that the apple did not fall so very far from the tree, though. Sullivan's mother was a CIA analyst in Russia in the 1960s before she settled down to start a family.)

Sullivan got his law degree at the University of Miami in 1993. A self-described early adopter, he was the first of his friends to get a computer and an e-mail account. In his first job at the Department of Justice in Miami, he convinced his superiors that the office should have an Internet connection.

He has been riding the Internet crime wave since 1997, when he moved to Las Vegas as a federal prosecutor. When the DOJ started a computer crime program, recruiting one prosecutor in every office to work on cybercrime cases, he volunteered and began working on early eBay fraud and software piracy cases. After Bob Mueller, now director of the FBI, started recruiting a high-tech team to work in the DOJ's Silicon Valley office in 1999, Sullivan jumped at the chance, putting him at the center of cybercrime during the Internet boom. In 2002 he went to eBay, where his security detail included the units PayPal and Skype. That's when he had to make a fundamental shift in his thinking—not just how best to prosecute criminals but also how much information to hold back from authorities to protect the rights of customers.

"Depending on the product, we had fundamentally different philosophical approaches to the law and user expectations around data-sharing with law

enforcement," he says. As one might expect from someone who had been a prosecutor a scant year before, Sullivan's relationship with law enforcement when he first joined eBay was cozy. In 2003 off-the-record remarks Sullivan made at a cybercrime conference were secretly taped and given to a reporter at Haaretz.com, the Israeli news site. Sullivan claimed that eBay's privacy policy was "flexible," allowing it to freely provide information to investigators—"no need for a court order," Sullivan said. Haaretz wrote an outraged report about eBay's collusion with Big Brother.

"With Skype we'd tell law enforcement to go through Luxembourg, and good luck with that," says Sullivan now. "But with eBay, if you were law enforcement investigating a seller, you didn't even need a subpoena. You could just ask for it on your letterhead and we would hand it over. Back then some people were just putting money in envelopes, sending it to eBay sellers and hoping to get their products. There needed to be an expectation that sellers were being scrutinized."

Sullivan says the experience of looking through different legal lenses in terms of what to give to law enforcement was "really helpful" when he came to Facebook in 2008, "where expectation of privacy is paramount and our philosophy has to be the Skype policy." He claims that "99.9% of the time" when Facebook resists a request, the government backs down.

While Sullivan appreciates the nuances around privacy in the context of free expression and communication, he appears to have little tolerance for claims to privacy when it comes to either fraud or the treatment of children. With the rise of Facebook credits—the site's monetary system, which requires users to use virtual dollars to buy goods in games and apps on the site—he will likely adopt the eBay approach. Those dealing in Facebook dollars can expect to be closely scrutinized.

IN DECEMBER THE RAPIDLY EXPANDING Facebook moved from Palo Alto to Menlo Park, into Sun Microsystems' old headquarters, once known as "Sun Quentin," after the notorious Marin County bayside prison. The sprawling campus is still under construction around us on this February morning, with workers carrying ladders and bulldozers preparing the intrabuilding walkways for

food carts and play areas. Since employees can't use the central paths, there are dozens of bikes outside each building for use on the paved "Hacker Way" road that circles the campus. "Even when they're finished, it won't look too sculpted," says Sullivan, gazing out the windows of Building 18 at construction equipment. "The unfinished look of our campus is a cultural thing."

Inside, the walls bear a passing resemblance to the scrapbook feel of profile pages. Prints from the videogame Donkey Kong and scrawled messages from visitors (many who thank Facebook for enabling them to "stalk" the man or woman who eventually became their spouse) hang alongside the security team's "scalps"—photos and investigation details for spammers, hackers and pedophiles hunted down and kicked off the site. The conference room names in the security building are mash-ups of music artists and security threats, such as "Alicia Keylogger." Sullivan gestures at ten people sitting at a row of desks, who smile shyly in our direction.

"They handle requests from law enforcement," he explains. The security team has five other members based in Dublin, Ireland who speak every European language and field government requests internationally. "Claudio, for example, speaks to every police officer in Italy and answers any question they might have about Facebook. We're very careful about the information we share, but that doesn't mean we can't help them understand the situation that they've never dealt with before."

WikiLeaks' Julian Assange has called Facebook the world's perfect spying machine, with access to 40% of the world's two billion Internet users. A 24-year-old Austrian law student recently took advantage of Europe's "right to access" law—which forces companies to provide all information they have on a citizen upon request—to get his Facebook file. After three years on the site it ran to an incredible 1,222 pages long.

Sullivan scoffs at the spying machine characterization. "We don't have a data pipeline to the CIA," he says. "If people had horrible experiences, they would stop using Facebook."

That echoes a sentiment expressed in the company's recent S-1 filing to go public: "Any number of factors could potentially negatively affect user retention, growth and engagement, including if there are changes in user sentiment about the quality or usefulness of our products or concerns related to privacy and sharing, safety, security or other factors."

Law enforcement, as well as civil litigants, increasingly rely on third-party companies like Facebook as a source of evidence in criminal investigations and lawsuits. It's the nature of the overexposed age that we make much more information about ourselves readily available and easily discoverable.

Sullivan goes over his most recent weekly security report to Facebook executives, in which he highlights significant incidents of ne'er-do-wells getting poked by the security team. Sullivan notes that Florida police called Facebook's 24-hour emergency hotline for law enforcement the previous week to request help locating a two-week-old baby who had been abducted from its mother. When law enforcement calls the hotline in a life-or-death emergency, Facebook waives basic legal requirements and hands over information to authorities without making them go through official channels. In this case it provided authorities with the IP address and location information for the last sign-in for the Facebook user suspected of abducting the child. The baby was recovered 30 minutes later.

In another incident, proactive policing by Facebook's security team led to a potential pedophile being fingered. The site employs algorithms to detect suspicious behavior and bring it to the attention of Sullivan's group. "We found that a youth pastor and children's sports coach in Indiana was using fake accounts to try to engage with kids on our site," he says. "So we called the FBI in Indiana and sent them his information."

While a youth pastor reaching out to young people doesn't seem particularly nefarious, Sullivan suggests that his use of fake accounts to do so, as well as the content of his communications, was disturbing enough to warrant police involvement.

Users may often forget they are constantly watched on the site, if not by actual people, then by algorithms. Last year Facebook adopted a Microsoft program called PhotoDNA, which scans every picture uploaded to the site to see if it matches known child porn images compiled by the FBI's National Crime Information Center. "Our list of child porn images is actually much longer than the FBI's," says Sullivan. "Every time we find something new—through a user report or flagging on a keyword—we manually review the user album to see if there are other images that should be added to the list, and then we add them to our library. We're exploring how to share our library with others."

For years the site has had back-end algorithms to weed out fake spam accounts and monitor kid-adult interactions. Lotharios, beware: "If you're sending friend requests that trend to 80% female, that's a red flag, or if you change your birth date a lot—under and above the 18 threshold," says Sullivan. "Our site integrity team has built engines to feed in characteristics, and they start hunting people down. When you have single concrete rules, it's easy for people to figure them out, but with machine learning, it's evolving all the time."

Sometimes in ways that most Facebook members probably aren't aware of. Sullivan's team determines when cops get to dig into users' accounts but also has the power to do its own snooping to prevent miscreants from abusing the site, as well as to turn those users over to authorities. The Constitution protects us against unreasonable searches by the feds, requiring them, for example, to get a search warrant from a judge to riffle through our digital homes just as they do for our physical ones. But when it comes to our privacy rights from the companies that store our data? That's more complicated.

Privacy—or the lack of it—is the biggest complaint about Facebook. Constant tinkering with privacy settings has prompted instant pushback from users and retreat by the company. After an investigation by the Federal Trade Commission into unfair and deceptive practices, the site is now subject to privacy audits every two years. That hasn't stopped a high recidivism rate. Recently, Facebook's switching all users over from their exiting profile pages to "Timelines" that expose

activity from years earlier by migrating it to the user's front page provoked an outcry from privacy advocates.

SINCE JOINING FACEBOOK Sullivan has brought a more confrontational approach to security on the site. While many companies focus on deterrence and eliminating threats, Sullivan also wants to pursue malefactors. "Joe is aggressive about going after bad guys," says Alex Rice, a member of his security team. "I attribute that to his prosecutor background."

Sullivan complains that law enforcement is too focused on intellectual-property crimes and takes little interest in malware and spam cases, a growing headache for social sites. So Facebook has taken matters into its own hands, pursuing suspects in civil court and in the court of public opinion.

"A lot of companies stop at playing defense, like credit card companies—they invest a lot in fraud detection and prevention, but they're not bringing civil actions," says Sullivan. "We spend a lot of time trying to figure out who's sitting on the other side of cybercrime."

One frequent scam involves tricking users into filling out surveys or visiting websites that generate profit for marketing firms, inducing them with promises of lurid images, often involving Justin Bieber. Facebook's lawyers hand out cease-and-desist letters like candy. When a site called IsAnyoneUp began taking screenshots of users' pages to post alongside naked photos of them, Facebook sent the purveyor a letter, shut down his account and took away his ability to install the "like" button on his site. (That still hasn't stopped him.) It has also taken to court dozens of spammers, as well as advertising and marketing outfits, under the CAN-SPAM Act, and has been awarded more than $1 billion in judgments.

"Security is so high on e-mail now," says Dirk Kollberg, a security researcher for Sophos in Wiesbaden, Germany. "Everyone knows to look out for spam and viruses there. But people are not educated about avoiding these things on social media, so that's where the criminals are migrating."

So, taking the law into its own cyberhands, Facebook is outing them. Collaborating with Sophos, the company fingered five Russians behind the Koobface worm that infected hundreds of thousands of computers and generated at least $6 million in criminal gains for its creators. When users clicked on “YOU HAVE TO WATCH THIS CRAZY VIDEO” Facebook posts, they were instructed to download an update to their software. The infected computers became unwitting slaves of a botnet ring run by the Koobface gang. They profited by hijacking Web searches to send users to rogue sites and bombarding users with ads run by other cybercriminals.

Sullivan went the extra step because he thought he had to. With Sophos he tracked digital bread crumbs to expose the guys responsible for Koobface (an anagram for Facebook). They gave their evidence to the FBI and waited for it to make a move. After over a year of inaction, though, they took a vigilante approach, exposing the gang members in the New York Times after a security blogger blew the whistle on one member, thus alerting the group they were being pursued. Facebook and Sophos detailed how they tracked them down using IP fingerprints, Foursquare check-ins, Twitter activity, friend lists on a Russian social networking site and Flickr photos that showed the gang vacationing in Europe. “It’s not about monitoring the users,” says Kollberg, who participated in the Koobface sting, “but producing security for users.”

Sometimes Facebook goes too far—then pulls back. While Sullivan won’t be specific, he cites the hypothetical case of teens using Facebook in a “spammy but borderline legal way”—say, by mass inviting people to events. In such instances his team usually doesn’t turn the offenders over to authorities but instead calls their mothers.

Unrestricted by constitutional restraints, “lawyers at Facebook and Google and Microsoft have more power over the future of privacy and free expression than any king or president or Supreme Court justice,” writes legal scholar Jeffrey Rosen.

Sullivan has harnessed crowdsourcing in service to vigilantism. He won a budget to institute a Facebook bug bounty program, where independent sleuths can earn

$500 or more for identifying (and keeping secret) security and privacy flaws on the site. “We have a very small security team,” he says. “So we’re trying to turn our users into patrol guards.”

Facebook has made that reporting process easy for users, including a “report” button on every piece of content that appears on the site, so that users can mark it as “spam or a scam,” “nudity,” “violence,” “hate speech” or a number of other categories. It has helped the company nab lots of high-profile bad guys. When a Chicago man posted a photo of his toddler bound and gagged with duct tape in December, captioning it, “This is wut happens wen my baby hits me back,” the photo was flagged. He was reported to authorities and charged with aggravated domestic battery.

But the community watch program can also backfire, especially when it tries to turn a miscreant into a do-gooder. In December a user discovered an Achilles’ heel in Facebook’s security and decided to go public with it, showing how you could expose a user’s private photos by reporting one of their public photos as “abusive”; Facebook then offered the user’s other private photos to flag any that were similarly abusive. The person who discovered the flaw posted it to the Bodybuilding.com message forum and included some of Mark Zuckerberg’s private photos exposed in this way. “My hope is that he just didn’t know there was a place he could go to make money for reporting a bug like that,” says Sullivan.

HOW DO YOU MAKE A SAFER, more law-abiding place without creating a stifling surveillance cyberstate? Now that Facebook has biometric face prints for hundreds of millions of users, what will it do when law enforcement comes with a photo of a criminal suspect and asks for an identification?

“We’d insist on a court order, and we’d fight it as far in the court system as we could go,” says Sullivan, adding that Facebook gets thousands of calls and e-mails from authorities each week. “Recently a government agency wanted us to start logging information we don’t log. We told them we wouldn’t start logging that piece of data because we don’t need it to provide a good product. We talked to our general counsel. The law is not black-and-white. That agency thinks they can compel us to. We told them to go to court. They haven’t done that yet.”

Still, the Fourth Amendment against unreasonable searches and seizures can't shield against these requests because of the so-called third party doctrine, which says the information you knowingly provide to a third party loses its privacy protections, making it much easier for the government to get your phone, banking and Internet records. In a recent Supreme Court decision Justice Sonia Sotomayor suggested the doctrine is "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." She suggested the doctrine be rethought.

The 1986 Electronic Communications Privacy Act puts up extra legal barriers around e-mail and other communication "content." It requires cops to get a warrant to get access, rather than simply asking companies to hand it over. But the feds have been pushing for easier access and looser regulations.

In such a fluid legal climate, how much can we trust sites like Facebook to safeguard our digital diaries that we willingly surrender to them? For Sullivan it's a matter of protecting users and the integrity of the site—and hunting down the bad guys, a vestige of his days at the DOJ. "As a prosecutor, you feel like you're always on the side of right."

I'm a privacy pragmatist, writing about the intersection of law, technology, social media and our personal information. If you have story ideas or tips, e-mail me at khill@forbes.com. PGP key MORE