Veneer of privacy grows thinner as technology infiltrates our lives

January 8 2014, by Lisa Krieger

We're no longer just strangers in a crowd. Imagine any street corner in any town where, let's say, four people - Alexandria, Larry, Cory and Cameron - are lost in private thought. Without a single conversation, without even knowing their names, we could learn that Alexandria's angry ex-boyfriend posted her photo on a "revenge porn" website. That Larry is mourning the death of his daughter. That Cory is trying to scrub her image from friends' social networks. That Cameron picked the wrong place to hide from police.

In each case, a simple photograph of the four strangers, combined with the power of data, opens the door to deeply personal details. That's one of the many ways digital technologies are turning our once-personal lives into a global show-and-tell and redefining our expectations of privacy.

Almost every day brings new revelations about how Big Brother snoops on us and Big Data mines our online activities for profit. Even so, we are only beginning to understand the power of these incursions. In a few years, our faces alone, snapped on a street, in a crowd, or posted by a friend on the Internet, will be the key for a search engine to reveal the stories of our lives.

There may be nothing that technology is changing more dramatically than privacy. What is happening with our images online is just one example of our digital reality: We're living life out loud - secrets and all.

To be sure, gossip is as old as our species. It spread through villages in

whispers or over our grandparents' "party line" phones. And the impulse to share photos of ourselves started the moment Louis Daguerre first fixed images onto sheets of silver-plated copper.

But information moved at a human pace - eventually forgiven, forgotten.

Now this information travels across continents with just a click. And it can remain virtually forever in the data stream. There is no "erase" key.

People like Alexandria discover that in new and shocking ways every day.

"I am flabbergasted. It is crazy," she said after a reporter discovered a topless photo of her on a pornographic website that her ex-fiance had posted more than two years after their breakup.

He has remarried and has a child; she is engaged. Yet the photo persists - and the Netherlands-based website demands $500 to remove it.

We're not publishing her name to avoid a further invasion of her privacy. She had no idea her bare-chested image was out there - with her name, hometown and age attached - until the reporter called. "It was a personal thing between me and him," she said. "It happened one time, and I didn't think he'd hold onto them."

(A similar California case led to criminal charges recently when the attorney general announced the arrest of a San Diego man accused of asking women for up to $350 each to remove illicit photos from another revenge site.)

Here is the simple math behind our brave new digital world, with its blurry boundaries between private and public: Photos (plus) name (equals) information.

Photos - a snapshot at a party or a "selfie" shot in the bedroom - can reveal names, using tools like Google Plus' "Find My Face" and Facebook's facial recognition software. And geo-tagged posts on social networks can reveal the precise location of your whereabouts.

Then our names become a pipeline to once-private information, such as home address, age, employment, taxes paid, political affiliations and campaign contributions.

Where is this headed? For better or worse, we're becoming one vast Neighborhood Watch. And the surveillance doesn't stop at front doors, but follows us inside.

We're not just living with Big Brother peering over our electronic shoulders. We're also a more tightly connected nation, with many fiercely committed busybodies.

There was a time when explicit or offensive images never made it out of the darkroom. "Back in the film days, it was never an issue. ... We just wouldn't make the print" if it crossed a line, said longtime photo processor Bill Graham of the Palo Alto, Calif., camera shop Keeble & Shucat.

Just the idea of a stranger at a film processing lab looking at our images filtered our photo impulses.

Now, millions every day rush to reveal pictures and more rush to view them and pass them along, sometimes with tragic results.

"You can do the stupidest thing, and pretty soon the whole world knows," said privacy expert Frank Ahern.

When Saratoga, Calif., teenagers shared their cellphone photograph of

student Audrie Pott after an alleged assault, the humiliation led to the 15-year-old's suicide, her parents say.

"These cellphones or other electronic devices that can take photos or send emails are, in essence, loaded guns," said her father, Larry Pott.

"They are unchecked and completely open for any sort of unchecked transmission," he said. "There is no accountability. They are completely anonymous."

It used to be expensive to make things public and cheap to keep them private, notes Internet scholar and New York University professor Clay Shirky. Now it's expensive and time-consuming to make things private. But it's cheap - and easy - to be public. About 2.5 billion people worldwide have a digital camera in their pockets, often attached to a smartphone, according to Hong Kong-based mobile technology consultant Tomi Ahonen. If each person snaps 150 photos a year, that adds up to a staggering 375 billion images annually.

San Francisco Bay Area resident Cory Colligan knows the challenge of protecting her privacy. When a friend tags her in a Facebook photo, she "untags" it, or politely emails a request to delete it. If feelings are hurt, she explains her concern to friends over lunch.

"I love social media, but I don't post photos. I don't want to be out there that way. Period. I'm a private person," Colligan said. So she decorates her Facebook page with inspirational messages and landscapes; only her professional LinkedIn profile has a photo.

But sharing photos through social media will escalate, experts say, because it fills a human need for connection and intimacy. They help us stitch together our communities, keeping us in closer touch with the people we love.

"Tools like Flickr reverse the old order of group activity - transforming 'gather, then share' into 'share, then gather,' " Shirky writes in "Here Comes Everybody," his book about the Internet and group dynamics.

To some, losing privacy is a small price for exchanged memories of high school pranks or photos of cherished newborns.

Los Angeles actor and director Justin Baldoni proposed to his girlfriend Emily Foxler in an online video montage of proposal parodies, an 'N Sync lip sync, a flash mob and a visit to her father's grave to ask permission to marry her.

By November, more than 7 million people had clicked on his YouTube public proposal.

Until recently, if we wanted to stay anonymous, photos were no real threat. But improving computer programs and a proliferation of surveillance cameras is changing that. Facial identification becomes easier as improved cameras create higher quality images. And cameras are getting cheaper - and smaller.

Facial recognition is already in some TVs. Passwords and PINs are giving way to faceprints in our mobile devices.

When you knock on a door, shop or drive down the street, chances are good that you're on camera.

The Boston Marathon bombers would famously discover that. And so did Cameron Conley of Oakland, Calif. He vanished, Palo Alto police said, after leading them on a wild chase through downtown, hitting six cars and allegedly attempting to carjack a truck. But a homeowner's surveillance camera revealed his location.

"It showed that the guy had entered our property, and never left ... He was huddled underneath the house, in a crawlspace," said homeowner Roberta Chew. "Without the camera, he would have totally gotten away with it."

Cameras increasingly serve as protective eyes and ears when we're not present. A camera in an Oklahoma City nursing home recorded an aide stuffing gloves into a 96-year-old dementia patient's mouth. Police who use cameras have fewer complaints against them and fewer false allegations of brutality.

But technology has moved up a notch to search out faces. No longer is it necessary to watch hours of surveillance video for a suspect or car. A computer program developed by the San Francisco company 3VR can quickly search huge quantities of video to find a specific face - matching gender, age and facial characteristics. It also can detect suspicious behavior - such as lingering - that the human eye might not notice.

But our images can turn up in ways never intended. Google Maps' satellite camera captured the body of Kevin Barrera, a 14-year-old Richmond homicide victim, haunting his family. The face of suicide victim Rehtaeh Parsons, 17, was featured in an ad on Facebook for a dating site, Ionechat.com, advertising "Find Love In Canada!"

Alexandria and other women suffer when X-rated photos, emails or texts are posted on niche websites - sometimes with the victim's personal information. Alexandria had puzzled over why she was receiving suggestive Facebook messages from strange men - and now she knows why.

Our faces can lead strangers to our names.

The U.S. State Department uses facial recognition software to link

passport photos and names, stopping fraud and fleeing criminals. The FBI runs the world's largest biometric database, housing not just fingerprints but also mug shots, tattoos and other identifying information for tens of millions of criminals, and more than 34 million civil fingerprints.

But police cameras can't compete with the vast social net that we unwittingly are weaving with our mug shots and names posted on Facebook, Instagram, LinkedIn and ordinary corporate and organizational rosters.

Facebook alone holds an estimated 90 billion digital photos. Profile pictures and names have no privacy settings. Neither do LinkedIn's profiles; its photos are associated with real first and last names available to casual visitors without logging on.

Facial recognition software finds us on Facebook every time it suggests "tags" for your face found in others' photos. Google offers Picasa users facial recognition tools to organize photos; Apple offers a similar tool to iPhoto users.

One researcher used photos to identify anonymous students - some down to the last four digits of their Social Security numbers. Alessandro Acquisti, an associate professor at Carnegie Mellon University, used just a consumer-grade digital camera, off-the-shelf facial recognition software and social network information to sift through Facebook profiles and other websites. He was able to identify many of them instantly and also obtain their personal data.

Learning our names opens the gate to a vast store of publicly available information - such as home addresses, voting records, campaign contributions, mortgages, liens and birth, marriage, divorce and death records. Some businesses, such as Intelius and Spokeo, sell this

information. Linked with consumer information - such as air miles, loyalty cards, magazine subscriptions and other purchases - our names gain added value. Companies like Datalogix, Epsilon and Acxiom auction off to advertisers access to us.

The day may be coming, experts say, when your phone's facial recognition software recognizes and identifies a long-forgotten friend, and also reveals your location to a stalker. A hotel will greet you by name, but a car salesperson may infer your credit score and download your psychological profile. A database will find missing children - but also identify the people attending a peaceful protest.

A fledgling but impassioned movement has risen to strengthen online privacy protections, using browsers like Mozilla Firefox, social network platforms like Ravetree, the search engine DuckDuckGo and photo-sharing services like Snapchat, which allows photos to quickly vanish.

Without changes, Acquisti foresees a "post-private" world where we'll no longer take risks and learn from mistakes. It will be a less creative and more cautious society, he predicts, "a very sad and creepy place."

But others argue that we are entering a new Age of Transparency, where increasing openness is healthy.

"Privacy is dead," said Nova Spivack, a technology futurist. "In fact, it has been dying a rather operatic death for over a decade."

We're building a more moral and perhaps even more forgiving world, he believes. "When you know that you can't hide, you become more responsible."

It is possible to find a middle ground between either extreme of disclosure, balancing the risks and benefits, said San Francisco social

media expert Trish Chan.

"We assume privacy is the most important need. But there are other needs to be satisfied, not just privacy - such as connecting with friends," she said.

"When I think about privacy, I don't know quite what it means exactly these days. Everybody is so out there."