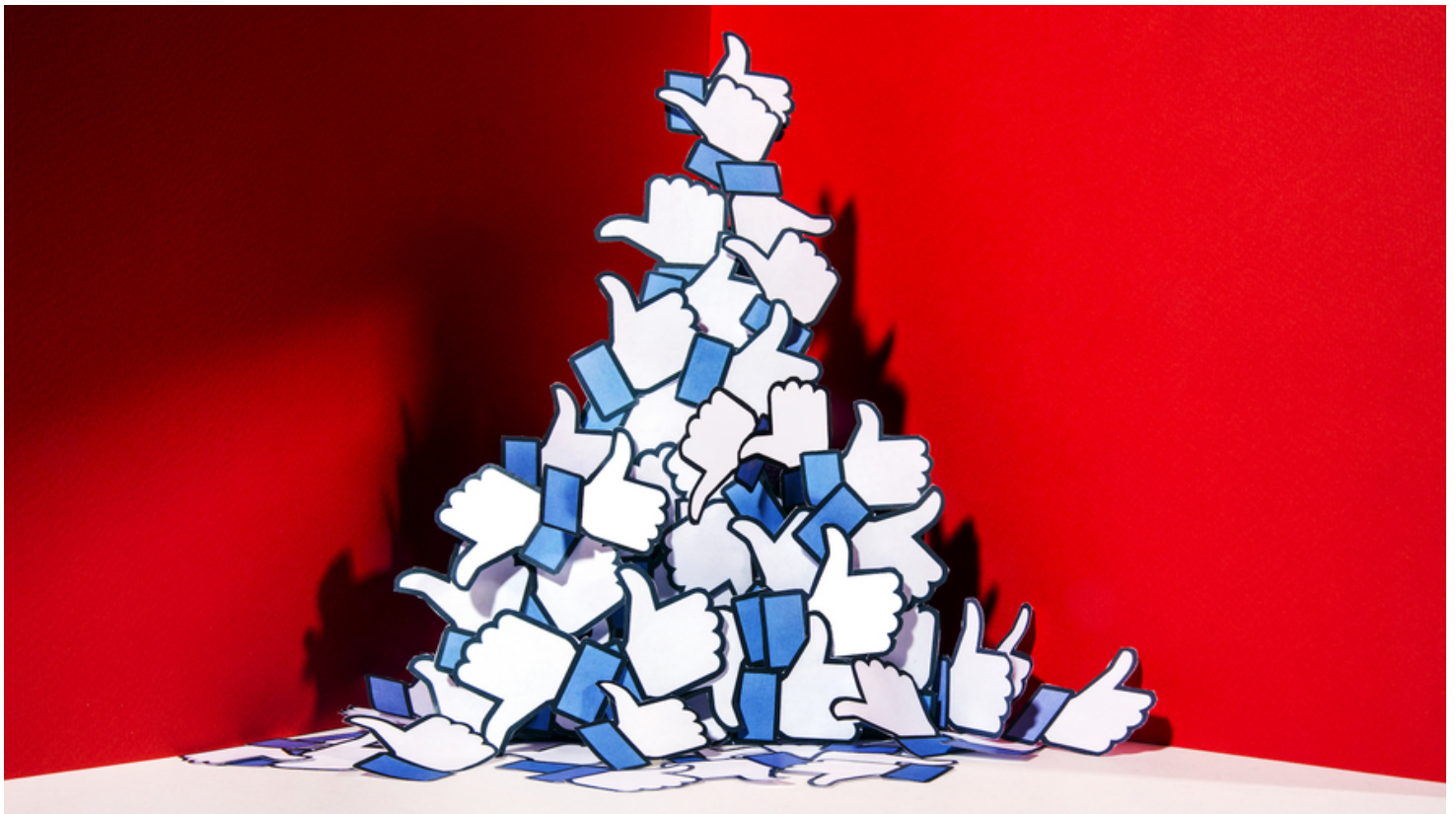# Start an online post, then delete it? Many websites save it anyway

By Drew Harwell, Washington Post on 02.06.19

Word Count **947**

Level **MAX**

Facebook got in trouble recently for saving copies of deleted photos that users posted, then decided to delete. Photo by: Washington Post/Getty Images

When a Facebook user starts to post a photo, but decides not to and cancels, the social network still keeps a copy — saving a memory of something the person chose not to share, or wanted instead to forget.

That fact surprised users on December 14, when Facebook announced it had not just saved those photos, but, for up to 6 million users, inadvertently exposed them to a huge group of third-party apps.

Yet it's not just Facebook holding onto the ghosts of our Internet pasts. Many websites start sharing or saving the text, photos or other information before we commit with a click of "Post," "Enter" or "Submit," and sometimes even after we choose to delete.

Many online users have a general sense that they're being tracked online — a long-lasting footprint of browser "cookies," website log-ins and search histories that can follow them around the Web.

That data can generally help speed up web browsing and allow websites to more precisely track a person for purposes of search or advertising.

But some websites go a step further, by allowing the company to see what its users are currently typing. LiveAgent, an online chat service that companies use for customer service, offers a "real-time typing view" of everything a customer writes before hitting "Send message," saying it will allow the representative to begin preparing a response quicker. "Customers will appreciate your quick and precise answers," the company's website says.

David Cacik, an official at Quality Unit, which develops LiveAgent, said companies get to choose whether they want to alert people that their typing is being watched, saying it's "up to them to inform their users."

Fewer people know about this special kind of "undead" data — discarded by the user, but still saved by the site. And experts say companies aren't doing enough to educate privacy-minded users already anxious about what they're leaving behind.

People "don't realize that apps can track not only what you post, but any activity on the app," said Tiffany Li, a fellow at Yale Law School's Information Society Project. "And if people don't know the risks, they haven't been well-informed. That's on the companies."

This data can help designers and engineers pinpoint what might have caused a user to get distracted, discouraged or annoyed enough to not finish their work. But it also opens the possibility that users will unthinkingly offer information they weren't ready to fully share, in the belief they were the only one looking on.

It's hard to know how many websites keep this stuff saved. But Princeton University researchers last year found that hundreds of websites recorded all of their users' mouse movements and typed text — without telling the users they were doing so — in such detail that a site could "replay" everything that a user had said or done.

This type of software was found on the websites of WordPress, Spotify, LiveJournal and many others, though the presence of it didn't mean everything was being recorded, and websites had a choice in whether to save the data. The tracking, researchers wrote, could expose users' medical conditions, credit-card details, passwords and other sensitive information to scams and identity theft.

Facebook said December 14 it had saved the photos that users abandoned before sending just in case users wanted to finish posting them later. And email services such as Google's Gmail and social-media sites such as Twitter automatically save "drafts" of what people typed for later sending or deletion.

But officials from Instagram and Twitter say they don't upload messages, photos or videos onto their servers until they're posted. The drafts are saved locally on the person's phone, and are viewable only by them. Instagram, which is owned by Facebook, also says it wasn't affected by that Facebook bug.

Retail websites have also for years stored similar data on abandoned online shopping carts — in which users said they wanted to buy something, but ended up not finishing the purchase. The sites

will often send reminder emails to nudge users into sealing the deal. "Why did you leave me?!" says one such email from BlackMilk, an online clothing store.

Not every company stockpiles its users' data. Snapchat, the video-sharing app in which most messages self-destruct, uploads content as an encrypted file to its servers once someone starts a message. But if that user has second thoughts before sending, the keys to decrypt it are never created, and the unsent message is deleted within 24 hours or less.

But peeking at unposted messages is not new territory for many companies, including Facebook. In 2013, two workers there compiled data from 4 million users on what they called "last-minute self-censorship" — status updates, posts or comments that were written, then deleted.

About 70 percent of monitored users, they found, had done so over a period of about two weeks, and that rate changed based on lots of factors, including the makeup of their friend groups. But the focus of the research was all business: With too much self-censorship, they wrote, the social network "loses value from the lack of content generation."

Even if users read the privacy policies — a rarity, since many are dreadfully long and technically complex — it's not always so clear that their unsent thoughts will be saved and stored. Facebook's data policy says, "We collect the content, communications and other information you provide when you use our Products," but doesn't specifically mention unsent photos or messages.

Users can delete their accounts, but there's no way to go in and re-delete what they've already deleted. "We store data until it is no longer necessary to provide our services and Facebook Products, or until your account is deleted — whichever comes first," the policy says.