Another Way Facebook Rapes You, Facebook, And Dating Sites, Embed 'Hidden Codes' To Track Who Sees And Shares Your Stuff

Zak Doffman
Zak Doffman Contributor
Cybersecurity
I write about security and surveillance.


uncaptioned

Getty

Facebook has become synonymous with privacy violations in the year since Cambridge Analytica came to light. Now in the same week that details of the record $5 billion FTC fine emerged, an Australian cyber researcher has reopened a years-old debate as to whether the social media giant is embedding "hidden codes" in photos uploaded by users onto the site.

"Facebook is embedding tracking data inside photos you download," Edin Jusupovic claimed on Twitter, explaining he had "noticed a structural abnormality when looking at a hex dump of an image file from an unknown origin only to discover it contained what I now understand is an IPTC special instruction."

Twitter

Jusupovic described this as a "shocking level of tracking," adding that "the take from this is that they can potentially track photos outside of their own platform with a disturbing level of precision about who originally uploaded the photo (and much more)."

The "IPTC special instructions" that Jusupovic viewed are essentially metadata watermarks that Facebook adds to tag the image with its own coding—those tags can be read later, enabling the "tracking" to take place. This is not new, and at a basic level not especially well-hidden either. It can be used to trace the ownership of images, to resolve copyright infringements, to provide enhanced user services. It can also be used to better target advertising and trace links between different users—I have an image, where did I get it from.

YOU MAY ALSO LIKE

According to one analyst, the metadata has been added since 2016 and "contains an IPTC block with an 'Original Transmission Reference' field that contains some kind of text-encoded sequence. This coding method lets Facebook "know it has seen the image before when it gets uploaded again," explained a user on Reddit. "It is yet another way to learn associations between people. Person 1 uploaded a bunch of the same photos Person 2 uploaded, let's show them both all the same advertisements!"

Another user on the same forum linked the coding to the current focus on the spread of fake news: "You download a meme from some account/page which is known to spread propaganda/hate speech etc. Now you think, hey let me just share this on WhatsApp on my family groups, because why not. Now, Facebook can easily tag you as a user who 'believes in that propaganda' and can sell that data to political parties or companies to target ads or more propaganda on you."

There is no active tracking implied here, the image does not contain a secret beacon of any sort. It is a hidden code that would allow another Facebook or third-party site with the right software to link the image back to its origins—obviously, more metadata can be added as an image travels, which has additional implications. Think of this like the UV marker pens used to mark possessions with zip codes in case they're stolen.

Not everyone is willing to play along with the Facebook scheme though. Twitter strips out the basic level of IPTC coding when images are posted on its site. But what remains unknown is

whether there are other levels of more advanced steganography (hidden data in media) used by Facebook. There are continual advances being made in hiding data in images, some for security and data protection, others to execute advanced levels of malware that can be virally shared across social media platforms.