



# Apple's IDFA Kill-Move is a Frontal Assault on Rogue Advertising Industry - part 2

Feb 6th 2021

---

Apple chief executive Tim Cook launched a stinging attack on ad-based social networks, arguing that such platforms were responsible for real-world violence and dehumanising consumers.

Quotes from Mr. Cook's address at the Data Privacy Day in Brussels on Jan 28th-

- "At a moment of rampant disinformation and conspiracy theories juiced by algorithms, we can no longer turn a blind eye to a theory of technology that says all engagement is good engagement"
- "What are the consequences of prioritising conspiracy theories and violent incitement simply because of their high rates of engagement?" asked Apple's boss. "A social dilemma", he thundered, "cannot be allowed to become a social catastrophe."
- Mr Cook noted the average smartphone app contains "an average of six trackers" to "surveil and identify users across apps, watching and recording their behaviour". He added: "Users may not know whether the apps they use to pass the time, to check in with their friends, or to find a place to eat, may in fact be passing on information about the photos they've taken, the people in their contact list, or location data that reflects where they eat, sleep or pray."

Apple's director of global privacy, Jane Horvath, said in a separate panel that the group would like the US to adopt a federal privacy law – modelled after Europe's General Data Protection Regulation that came into effect in 2018. She said society had reached "an inflection point" in which people had to decide whether trading privacy for "free" services was worth the cost. "Some say that advertising may suffer without all of that data," she said. "We reject that you can't reset the privacy paradigm and still have a robust advertising ecosystem."

## **HISTORICAL CONTEXT**

Mr Cook's righteous wrath makes it easy to forget how in the early days, Apple enabled ad tracking. In the 2000s app developers and advertisers learned to use its

"unique device identifiers" to follow users around the internet. These UDIDs, as they were known for short, were permanently attached to every iPhone or iPad and made it easy to keep tabs on individuals' online activity. Then in 2010 a privacy furore erupted around Apple and Google. Two years later Apple responded by banning app developers from using UDIDs. For a brief few months advertisers could barely track its customers at all. The sixth incarnation of IOS introduced a new, less intrusive tool called "identifiers for advertisers". Unlike UDIDs, these can be blocked, and do not identify users personally; any data collected are aggregated before being used. But they still allow tracking, which is switched on by default on iPhones, and fiddly to turn off. Apple's aim back then was to help app developers earn revenue in IOS.

Now privacy is more central than ever to Apple's brand. Four years ago it stopped tracking users on Safari, its web browser. Google, too, has announced plans to eliminate third-party tracking "cookies" from its Chrome browser by 2022.

Ad-industry insiders find it odd that identifiers for advertisers are still around; last year some in the mobile-ad industry reckoned Apple was going to kill them off.