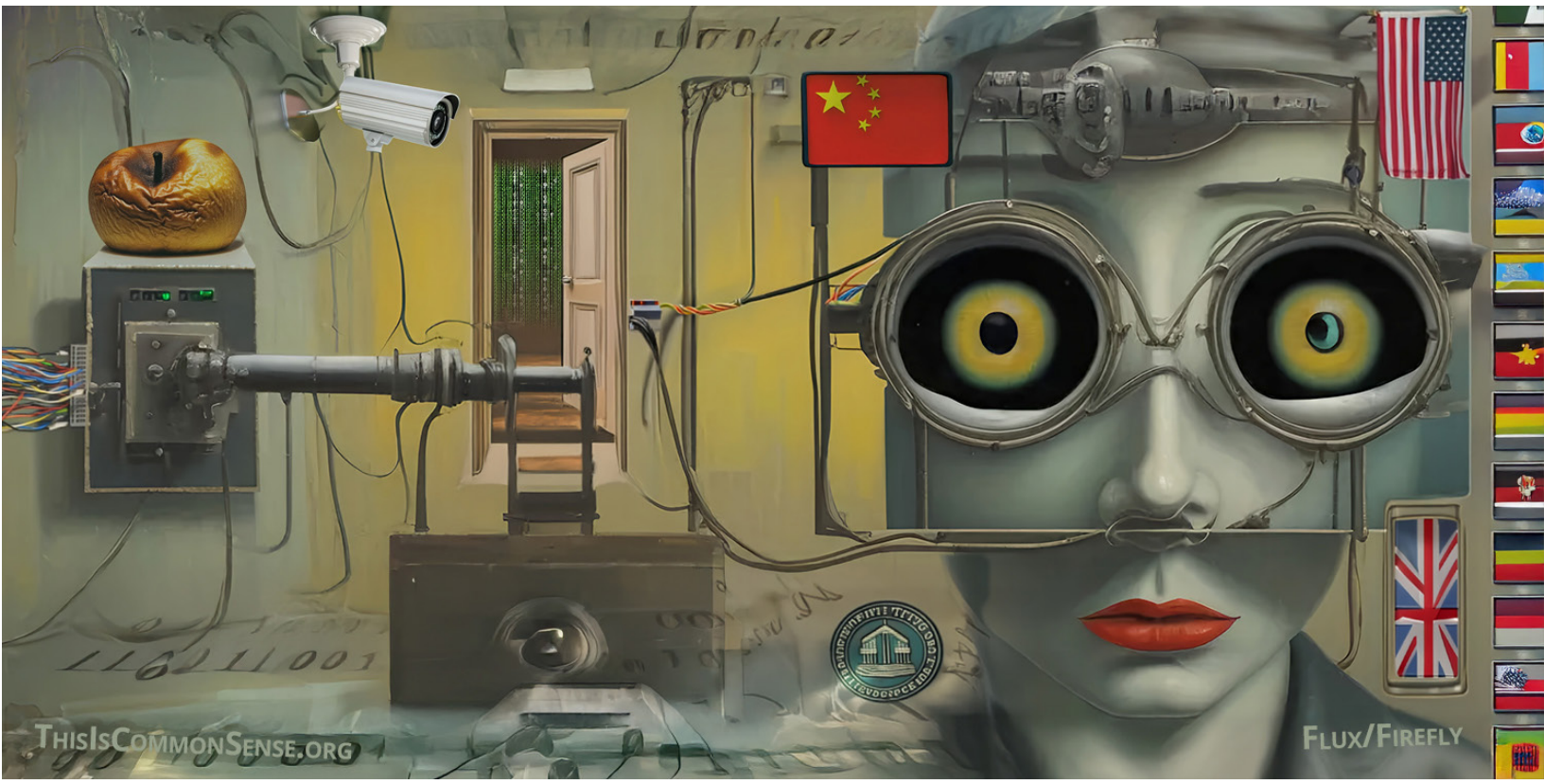

Tearing Into the Apple

February 11, 2025

"Any kind of back door … access for the 'good guys' can also be exploited by the 'bad guys,'" observes a Technology & Innovation Foundation report.

We can omit the skeptical scare quotes around "bad guys"; cyberhackers stealing your private information are bad guys.

Example: the China-affiliated hackers who looted U.S. telecommunications systems with the help of U.S.-mandated back doors.

But "good guys" demanding unlimited access to encrypted information are also bad guys.

Example: the United Kingdom officials behind a secret order last month, recent divulged by the *Washington Post*, demanding that "Apple allow access to all cloud content from users worldwide."

Reporter Joseph Menn observes that this hitherto undisclosed order requiring "blanket capability to view fully encrypted material, not merely assistance in cracking a specific account, has no known precedent in major democracies."

Apple is not commenting, now, to avoid legal jeopardy. But in March, when told the order was impending, Apple said: "There is no reason why the UK should have the authority to decide for citizens of the world whether they can avail themselves of the proven security benefits that flow from end-to-end encryption."

Apple may stop offering encrypted storage in the UK rather than obey the order. This probably wouldn't satisfy the Starmer government. If Apple sticks to its guns, its products may even end up being banned in the UK.

The alternative is open season for private and state-backed cyberhackers.

Meanwhile, time to remove your secrets from the cloud.

This is Common Sense. I'm Paul Jacob.