What is GCHQ?
Government Communications Headquarters is the security agency responsible for providing communications intelligence to the UK government.

What is the NSA?
The National Security Agency is responsible for collecting and analysing intelligence information and data in the USA.

Are governments spying on me?
If you use the internet or a mobile phone, the answer is probably 'yes'. Secret government surveillance Programmes like Prism and Upstream (run by the NSA) and Tempora (run by GCHQ) are believed to spy on you both by obtaining data from Google, Microsoft, Facebook and other major Internet companies, and by directly tapping into fibre-optic cables that carry global internet communications. The breathtaking scope of these programmes and the way in which global electronic communications are routed mean that people in nearly every country on earth can be spied on.

What data are they collecting?
The NSA and GCHQ have powerful surveillance programs that store and analyse people's browser history, internet searches, emails, instant messages, webcam conversations and phone calls. They also collect metadata, or 'data about data', which includes email recipients, call times and location records.

Which federal agencies use social media monitoring?
Many federal agencies use social media, including the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Department of State (State Department), Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Postal Service (USPS), Internal Revenue Service (IRS), U.S. Marshals Service, and Social Security Administration (SSA). This document focuses primarily on the activities of DHS, FBI, and the State Department, as the agencies that make the most extensive use of social media for monitoring, targeting, and information collection.

How can the government's use of social media harm people?
Government monitoring of social media can work to people's detriment in at least four ways: (1) wrongly implicating an individual or group in criminal behaviour based on their activity on social media; (2) misinterpreting the meaning of social media activity, sometimes with severe consequences; (3) suppressing people's willingness to talk or connect openly online; and (4) invading individuals' privacy.

Who is harmed by social media monitoring?
Echoing the transgressions of the civil rights era, there are myriad examples of the FBI and DHS using social media to surveil people speaking out on issues from racial justice to the treatment of immigrants. Both agencies have monitored Black Lives Matter activists. In 2017, the FBI created a specious terrorism threat category called "Black Identity Extremism" (BIE), which can

be read to include protests against police violence. This category has been used to rationalise continued surveillance of black activists, including monitoring of social media activity. In 2020, DHS's Office of Intelligence & Analysis (I&A) used social media and other tools to target and monitor racial justice protesters in Portland, OR, justifying this surveillance by pointing to the threat of vandalism to Confederate monuments. I&A then disseminated intelligence reports on journalists reporting on this overreach.

Can the government access my camera?
Yes, the government can access your camera in certain circumstances, but it's not common. The government typically needs a warrant from a judge to access your device.

What information does the NSA collect?
A record of most calls made in the U.S.
Email, Facebook posts and instant messages.
The contents of an unknown number of phone calls There have been several reports that the NSA records the audio contents of some phone calls and a leaked document confirms this.

Does the NSA record everything about everyone, all the time?
The NSA records as much information as it can, subject to technical limitations and legal constraints. This currently includes the metadata for nearly all telephone calls made in the U.S. (but not their content) and massive amounts of Internet traffic with at least one end outside the U.S.
The collected information covers "nearly everything a user does on the Internet," according to a presentation on the XKEYSCORE system.

Does the NSA need an individualised warrant to listen to my calls or look at my emails?
Not in all cases. Leaked court orders set out the "minimization" procedures that govern what the NSA can do with the domestic information it has intercepted. The NSA is allowed to store this domestic information because of the technical difficulties in separating foreign from domestic communications when large amounts of data are being captured.

How long can the NSA keep information on Americans?
The NSA can generally keep intercepted domestic communications for up to five years. It can keep them indefinitely under certain circumstances, such as when the communication contains evidence of a crime or when it's "foreign intelligence information," a broad legal term that includes anything relevant to "the conduct of the foreign affairs of the United States."