BIG BROTHER WORKS BOTH SIDES OF THE ATLANTIC

I was rather surprised that there seemed to be more outrage Sunday about the UK's announced plan to roll out the same ability to monitor everyone's online activity that the US set up after 9/11 then over Eric Lichtblau's report—based on the ACLU's FOIA efforts—revealing that cops all over the country are using our smart phones to spy on us.

At least from the published reports, it sounds like the Brits want to be able to do through GCHQ what NSA and FBI have been doing with hoovered telecom records for years.

> A new law – which may be announced in the forthcoming Queen's Speech in May – would not allow GCHQ to access the content of emails, calls or messages without a warrant.
>
> But it would enable intelligence officers to identify who an individual or group is in contact with, how often and for how long. They would also be able to see which websites someone had visited.
>
> [snip]
>
> "What this is talking about doing is not focusing on terrorists or criminals, it's absolutely everybody's emails, phone calls, web access…" he told the BBC.
>
> "All that's got to be recorded for two years and the government will be able to get at it with no by your leave from anybody."
>
> He said that until now anyone wishing to monitor communications had been required to gain permission from a magistrate.

Plus, such plans will likely face more of a hurdle in Parliament than such schemes to expand surveillance face in Congress.

Meanwhile, the materials collected from all over the country via ACLU's state affiliates show that local police are using some of the same approaches—things like communities of interest—that our massive data collection supports.

And as ACLU's summary makes clear that not just the Feds using Secret PATRIOT, but local cops, are using cell phones to track people with no warrants.

> **Most law enforcement agencies do not obtain a warrant to track cell phones, but some do, and the legal standards used vary widely.** Some police departments protect privacy by obtaining a warrant based upon probable cause when tracking cell phones. For example, police in the County of Hawaii, Wichita, and Lexington, Ky. demonstrate probable cause and obtain a warrant when tracking cell phones. If these police departments can protect both public safety and privacy by meeting the warrant and probable cause requirements, then surely other agencies can as well.
>
> Unfortunately, other departments do not always demonstrate probable cause and obtain a warrant when tracking cell phones. For example, police in Lincoln, Neb. obtain even GPS location data, which is more precise than cell tower location information, on telephones without demonstrating probable cause. Police in Wilson County, N.C. obtain historical cell tracking data where it is "relevant and material" to an ongoing investigation, a standard lower than probable cause.
>
> **Police use various methods to track cell phones**. Most commonly, law enforcement

> agencies obtain cell phone records about one person from a cell phone carrier. However, some police departments, like in Gilbert, Ariz., have purchased their own cell tracking technology.
>
> Sometimes, law enforcement agencies obtain all of the cell phone numbers at a particular location at a particular time. For example, a law enforcement agent in Tucson, Ariz. prepared a memo for fellow officers explaining how to obtain this data. And records from Cary, N.C. include a request for all phones that utilized particular cell phone towers.

Of course, all this cell phone tracking was—to some degree—available via FOIA. The Feds have far greater financial resources to do this tracking, and (in the counterterrorism realm) they do it in secret.

And if the response is any indication, folks care more about the Brits matching our surveillance than the way even our local cops have turned our cell phones into tracking devices.