

**I asked:** ok now what if that fake session id was inserted a row into of a fabricated table placed in the website's database and passed off as a legitimate part of the website's schema. does that change anything?

**Yes — that changes *everything*.**

At that point, what you're describing isn't merely a matter of an "investigative technique" being hidden or a prosecutor giving a misleading explanation — it crosses into *evidence fabrication*, *tampering*, and potentially *fraud upon the court*.

Let's go carefully and systematically.

---

### 1 What you're describing, technically

If law enforcement (or someone acting under their direction)

- \* *inserted a fake table* into the website's database, and
- \* *added a row containing a fabricated session ID*,
- \* *then represented that table and its contents to the court or defense as native, legitimate website data*,

then this is not a "tracking technique." It's *data falsification inside a target system* — a deliberate act that changes what the evidence *is*.

That's not a passive or covert observation method (like packet capture). It's an *active alteration* of evidence.

---

### 2 Legal and constitutional implications

Issue	Explanation
Evidence fabrication	Knowingly inserting or altering data to create false evidence is classic fabrication. Under <i>Mooney v. Holohan</i> (1935) and <i>Napue v. Illinois</i> (1959), using fabricated evidence violates due process.
Prosecutorial misconduct / Brady violation	If prosecutors knew the data was inserted and failed to disclose it, that's a due-process violation and potentially a violation of professional conduct rules.
Search & seizure violations	Modifying the contents of a target database exceeds the authority of a Title III wiretap or a search warrant, which allow interception or copying, not insertion or alteration.
Chain-of-custody issues	Any digital evidence extracted from that database would be unreliable and subject to suppression.
Fraud upon the court	Submitting altered data as authentic website content undermines the integrity of the judicial process. Courts treat that as a grave matter; it can justify dismissal or vacatur.

So yes — this changes the nature of the act from \*concealment of a technique\* to \*affirmative falsification of evidence\*.

### 3 Relation to FOIA Exemption 7(E)

At this point, 7(E) becomes irrelevant as a legal shield.

\* 7(E) is designed to protect investigative \*\*methods\*\*, not to conceal \*\*misconduct\*\* or \*\*forgeries\*\*.

\* Courts have held that FOIA cannot be used to “perpetuate a fraud” or hide illegal actions; if a document’s contents reveal government wrongdoing, exemption claims lose legitimacy.

If the government used 7(E) to mask the insertion of fabricated data, that would itself constitute \*\*bad-faith use of FOIA exemptions\*\* — something that courts can sanction if proven.

### 4 Practical implications

If such fabrication occurred and was used in an indictment:

\* The indictment could be subject to \*\*dismissal with prejudice\*\* if the fabrication was material to probable cause.

\* Any conviction based on that data would be vulnerable to \*\*reversal or vacatur\*\*.

\* Individuals involved (agents, prosecutors) could face \*\*professional or even criminal consequences\*\* if it was intentional.

Documentation would be critical: e.g.,

\* database schema comparisons showing the added table,

\* server-side code proving the site never generated those session IDs,

\* contemporaneous records or FOIA releases showing who had access.

### 5 Bottom line

Dimension	Consequence
**Nature of act**	From “withholding technique” → to “evidence fabrication.”
**7(E) protection**	No longer applicable; FOIA cannot shield falsified evidence.
**Criminal impact**	Potential due-process violation, grounds for dismissal or reversal.
**Ethical impact**	Potential prosecutorial and investigative misconduct.

In plain terms:

> If law enforcement inserted a fake table and fake session IDs into a website’s database, then represented that as authentic evidence, that’s not a legitimate law-enforcement method — that’s tampering. FOIA 7(E) cannot lawfully be invoked to conceal it.