

6. Risk of Meta-Data being hacked due weak Security Infrasture

[Return to Question 11](#) [Provide Feedback](#)

Metadata is data about data. Although this data can provide specific insight into personal data such as **Personal Identifiable Information (PII)** (see [Privacy Concerns](#)), there is also a problem with hackers gaining access to Metadata.

For example, knowing your name, address, phone number, and credit card details can be used to make illegal purchases in your name. This is a **Criminal Activity** in itself, but gaining information about your behavior and habits is a different kind of privacy violation. This information can be used to target you for advertisements or more nefariously specific scams. For instance, the metadata can now be used to determine that an individual is visiting a well-known cancer clinic and target the person for “miracle cures”.

Another example might be the discovery that a well-known founder and CEO of a publicly-traded company has visited the same well-known cancer clinic. This information is then used to in essence glean insider information about the company and make stock trades.

The use of Metadata is the primary engine for companies such as Google, Facebook, Microsoft, Apple, etc. However, this is done using their own mechanism to collect the data and users sign their rights away with the Service Level Agreements (SLAs), etc they “sign” when they choose to use these products. It is another thing to use government-provided data.

Therefore, Metadata not only contains Data about Data, but it can also contain information about the association of data elements together. Sometimes this activity is referred to as Triangulation.

Metadata Triangulation describes taking two pieces of metadata to infer a great deal more. Let me give you an example. You take a picture of something with your iPhone. That picture has both a date/time stamp and a GPS location tag. Two different pieces of information that, when combined, can lead to so much more. Some examples of information that can be inferred are:¹⁾

- The weather
- Top news stories (including the content of those stories)
- Local objects, buildings, structures, etc.
- Natural disasters
- Nearby housing prices
- Stock prices, economic conditions, inflation, etc.
- Flights overhead, traffic conditions

There is an assumption that Bitcoin transactions are anonymous, the reality is that they are anonymized. The following article by John Bohannon highlights the issue:²⁾

Bitcoin, the Internet currency beloved by computer scientists, libertarians, and criminals, is no

longer invulnerable. As recently as 3 years ago, it seemed that anyone could buy or sell anything with Bitcoin and never be tracked, let alone busted if they broke the law. "It's totally anonymous," was how one commenter put it in Bitcoin's forums in June 2013. "The FBI does not have a prayer of a chance of finding out who is who."

The Federal Bureau of Investigation (FBI) and other law enforcement begged to differ. Ross Ulbricht, the 31-year-old American who created Silk Road, a Bitcoin market facilitating the sale of \$1 billion in illegal drugs, was sentenced to life in prison in February 2015. In March, the assets of 28-year-old Czech national Tomáš Jiříkovský were seized; he's suspected of laundering \$40 million in stolen Bitcoins. Two more fell in September 2015: 33-year-old American Trendon Shavers pleaded guilty to running a \$150 million Ponzi scheme—the first Bitcoin securities fraud case—and 30-year-old Frenchman Mark Karpelès was arrested and charged with fraud and embezzlement of \$390 million from the now shuttered Bitcoin currency exchange Mt. Gox.

In this case, it was the “good guys” who used the Metadata, but this could also have been used for nefarious activities and a U.S. CBDC needs to protect this kind of data.

1)

Aaron Edell, Coining a term: metadata triangulation, 11 February 2016, Accessed: 24 April 2022, <https://www.linkedin.com/pulse/coin-ing-term-metadata-triangulation-aaron-edell/>

2)

John Bohannon, Why criminals can't hide behind Bitcoin - Even with cryptocurrency, investigators can follow the money, Science, 9 March 2016, Accessed: 24 April 2022, <https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin>

From:
<https://www.omgwiki.org/CBDC/> - OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki

Permanent link:
https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc_omg:04_doc:20_comments:brp:q11:06_risks&rev=1652751860

Last update: 2022/05/16 21:44

