

- What does it mean to be visible?

Being “visible” indicates a public, verifiable identity and traceable actions

- How is technology making it harder to “disappear”?

Because technology associates the individual with their online accounts and many other data points including usage data like IP addresses and device characteristics which can be verified as belonging to an individual, in addition to the data points which very easily attach a person’s real-world identity to their online account such as a mobile phone number. This blurs the line between physical identity and online identity, and because once something is public on the internet there’s basically no way to remove it, as it’s been archived and downloaded to multiple databases, caches, etc., the user is permanently made visible.

- Is technology making it easier for someone (or something) to “disappear” you? Explain with an example

For better or for worse today it’s nearly impossible to “disappear” someone living in a developed economy now as in addition to their physical presence they also have a paper trail consisting of lots of legal documents, business paperwork, timesheets, government ids, criminal databases, etc. along with every single online interaction they had. And now a person doesn’t even have to travel internationally in order to have their information overseas and out of control of their government. For example I host my website and personal projects in the EU, work for companies around the world and have travelled overseas despite being a native US citizen. The only viable entity who could “disappear” me would be the US government, but they would have to defeat a massive papertrail owned by hundreds of entities around the world. Fortunately however I make it somewhat easier by not using my photograph and using false information in some cases to protect my identity... but these are relatively insignificant.

- TO what extent do we control our “right to privacy” making this we “own” public or private at our discretion? Explain with an example.

We have no control over this. Despite the EU passing it’s honorable right to disappear act which requires companies to truly delete user data upon request, this system is flawed in that their data is being scraped on a regular basis by 3rd parties and even government actors. For example I worked with a company which was scraping data from instagram into a database and on a regular basis I noticed that accounts which had been scraped changed from public to private or were deleted/banned but their content survived in the database. Further I’ve made my own projects and seen primarily chinese and russian owned bots scraping my server looking for ways in and tracing my websites, likely adding them to a database as well. So in summary, we have no control in this case apart from maybe leaving to another country and abandoning the internet at a young age.