Public, Private, or Anonymous

In the pre-internet days, we all had a clearer understanding of the difference between public, private, and anonymous data. Putting aside special cases involving copyrights, trademarks, trade secrets, libel and pornography – we are able to focus on traditional facts that can easily be segmented into these categorizations.

Public data would be information on roadside billboards that you (and everyone else) could see driving down the highway. Now to me, growing up in the northeast and driving to see relatives in the south, the Stuckey's signs were the personification of public data:

For what looks like a simple sign with a simple message, a tremendous amount of information is conveyed in a manner that all of us are free to make use of for any lawful purpose. There is location information, time information, brand information, inventory information, price information and interestingly enough the tantalizing notion of "State Gifts" which to me was a code word for being able to buy things like fireworks that were illegal elsewhere. Nobody controlled who could access or use this information – and it would be absurd to think that someone could be in trouble for doing so. Nor did it matter whether I wrote this information down with pen and paper, or used a technological automation mechanism such as a Polaroid camera to capture the information for later use. The method of collection does not extend or restrict the right of collection, and the right of collection was universally understood to be absolute.

And the realm of what information was considered private was equally clear too. If I mail-ordered something that I might be embarrassed about (like a subscription to Playboy magazine), it would arrive in a plain brown wrapper so nobody, not even the mailman, knew what was coming to me. My trust in privacy would feel breached if the publisher released my name to others or publicly, or if the postman or my mother took a peek in the envelope, or my room was searched without due process of law.

And the definition of anonymous was the easiest of all – any transaction with a stranger or any retailer where you shopped infrequently enough that folks didn't remember you. Each dollar and coin was trusted enough to enable payors and payees to interact without the need for identity credentials to be exchanged. Unless I was buying a restricted item (i.e. a gun in most countries), the exchange of cash for goods or services could and would usually be anonymous in a retail setting or for a Craiglist consummation.

Life was simple and made sense. Public facts like in the Stuckey's ad were speech – essentially free speech protected by the First Amendment and as such equally open and available to all. Private information constituted the property of the individual(s) concerned, and breaches of privacy to the private could be punished by civil, and in some cases criminal laws. If there was more than one party to the private information then each party had a duty to protect that information from exposure to an unauthorized third person. And cash and coins were pretty much untraceable other than for edge cases like "bait money" given to bank robbers in the hope that a range of serial numbers would show up at identifying retailers or banks after the heist to provide clues to the identity of the perpetrators.

But post internet and post blockchain, the definitions and expectations around public, private and anonymous data have changed. We still have billboards in the form of web browsers for viewing information like a public facing LinkedIn or Craigslist posts, but the operators of those sites have treated access to and use of that publicly-available information as a property right that includes the power to exclude persons or entities from accessing or using the speech in those posts. Furthermore, LinkedIn and Craigslist have taken the position that they (rather than the authors of the posts) own the right to determine who can access and how they can use public data. It would be like the company that built the billboard or owned the land adjacent to the highway having the power to determine which occupants in the cars passing by could view or record details about my beloved Stucky's. The LinkedIn/Craigslist argument is that because the public data sits on private computers, the rights of the computer owners trump the First Amendment right of open and equal access to publicly available data. And the current threatened penalty for persons seeking unfettered access to such public information is felony prosecution for a hacking offense.

The notion of private information has also drastically changed in the era of search engines and social networks. Google and Facebook track your clicks and process what you are looking at. While they don't sell that specific information tied to your specific identity, they do remember your patterns and categorize that information so that search results and of course ads can be tailored to you. They do us this favor so that they can be more "helpful" in bringing us content that we've shown ourselves more amenable (or susceptible) to. Rather than all of us seeing the same ads on a TV show or finding the same books at a public library, we get tailored ads and our own private library of search results. Right wingers get more right wing ads and search results and left wingers get the same self-referential echo chamber results. The phenomenon accentuates the differences within and between us rather than coalescing on the commonalities. No wonder we end up living in separate realities both as individuals and as a country.

We also now have the nebulous notion of "semi-private" whereby we share something to a social media group of friends or followers. That might be 3 people or 300,000 people … but the supposed intention is that you are part of a select group getting this shared information. Of course there's nothing stopping anyone of those people from re-posting the shared semi-private information publicly for all to see. And there is a belief amongst some people, including the President of the United States, that if you revoke a tweet to your followers it's like you never said the words in the first place – even if has become part of the public record and discourse. The world has to rely on technology such as the Wayback Machine to see who said what and when as a matter of record. Otherwise, we live in a perfect Orwellian world where history can be changed with the press of a button so as to control the present and future.

And the creation of blockchain technology and the notion of digital cash, in the form of bitcoin and other alt coins, has transformed our understanding of anonymous data and payments. Though there has been a huge knock against these new forms of money as being out of the control of countries and regulated institutions, and therefore a conduit for black markets, the reality is different. Unlike cash, which is truly anonymous, the public nature of the blockchain means that any movement of value is only pseudo-anonymous. While the identity of the sender and receiver is not attached to the transaction, the full history of all the movements and associated patterns is completely and publicly available for all to see. Like a jigsaw puzzle, which one can start with just a few easy pieces to connect together, one can eventually sleuth together the degrees of separation to eventually make very good inferences as to the sources and uses of funds associated with this new technology. What may feel very anonymous at the time of transaction could be the electronic equivalent of bait money that historically ensnared bad actors in the past. The perpetrators of Silk Road did get caught quite easily and so, too, did the crooked federal agents that were shaking down the founder.

So, how and what should we want in this new world. I can't speak for others, but I can speak for my own desired shoulds and should nots. My belief is that while technology may have changed the scale and pace of everything, the underlying principles associated with our notions of public, private, and anonymous should not change in a way that compromises traditional protections for free speech, or that leaves any of us less empowered nor our society more divided. To that end, I propose the following principles as applied to our new technological circumstances.

i) Public facts are speech, not property. Therefore operators of publicly-available websites should not be allowed to discriminate as to who can access and use data contained within. Doing so would be a violation of the First Amendment and fair competition laws. The abuse of hacking statutes to punish parties accessing public facts is shameful and any Terms of Use that attempts to engage in such tactics should be deemed unenforceable.

ii) Users should be able to opt out of having their search clicks and social media information used to create an echo chamber of search results and ads that mirror back existing preferences and prejudices. We should be able to choose a neutral

existence on the web where data about our behaviors does not turn us into a segmented product living in a segregated reality.

iii) Our transactional activity should be able to be conducted through proxies that allow a level of indirection so that our behavior can remain anonymous to the viewing world. Only where the person or entity has cleared traditional safeguards, such as the necessity of obtaining a search warrant or court order, should our actual identity be revealed through (selectively) uncloaking the true identity behind underlying transactions. Privacy and security can be complementary rather than competing values.

iv) We should be able to execute our intent and consent to share our private information with whomever we so choose. Regardless of whether our data sits at a social network or a bank, we should enjoy an unencumbered right (through APIs or screen scraping if need be) to share that data with whomever we so choose without worrying about some internet provider claiming that they (not us) have the right to restrict the dissemination of our data. Interference in that right is a violation of a human right to control the disposition of our own personal data, which is our own property and should not be made subject to legalese buried in Terms of Use that nobody reads.

v) We all should be able to voluntarily allow a risk profile composed of attestations about the trust level in our identity to become a public record – equally and openly accessible to all. Without revealing the private information associated with these attestations, but rather only the level of identification and verification that has been achieved, we can all maximize our liberties (the permission to act) without overly burdening the party that needs to authorize us to enjoy the freedoms we seek. The risk profile should be controlled by us, rather than others (i.e. a credit bureau) with all references signed voluntarily by us (and co-signed by any mutually consenting third party).