10. Anonymous Identifiers

I know where you live.

This statement implies a threat that any failure in interaction can be met with an expansion beyond the scope of the transactions. That is a mouthful for your average bully. But the simple threat above is based on spheres of activity.

"Anonymous" is the opposite of "uniquely identified." A face in the crowd is anonymous depending on the size of the crowd and the feasibility of the technology to examine the crowd given its size. Today, a face in the crowd will be identifiable to the extent that there is video technology, and the individual facial geometry is recorded and unique.

Anonymity is the opposite of identity. Yet anonymity does not mean that there is no accountability. This is most richly explained in the scenarios. in chapters 14 through 17. Anonymity means that credential authentication does not depend on the intermittent step of identity authentication.

Cookies can be anonymous or function as identifiers. Cookies can be totally anonymous, linking only one request for information to the next.

The inherent value of the cookie itself is its functional: cookies save state. The cookie distinguishes each browser from the other. Without cookies, it would be impossible to fill a virtual shopping cart and then pay for the goods, as the thread of browsing connections over time would be lost.

When your cookie is linked to purchases and records from one site to another site, then that cookie subverts your anonymity by making connections across domains.

A cookie linked to your New York Times subscription registers on-line reading habits, as does one from Washington Post. That cookie may be linked to personal data entered during registration. That would make the cookie closely associated with personally identifiable information. However, entering one of the well-known and widely shared identifiers based on a favorite blog, a local soccer club or just a common well-known login also yields an identifier. In this case the identified is an *anonym*, instead of an I.D. It links your reading habits to others with the same ID, but you each have a unique cookie. Using these group identifiers is an expression of a desire for privacy.

A cookie that is linked to widely used ID identifies you as part of a statistical group. A blog, it identifies the number of readers who come from the blog and stay. In the soccer club, it identifies everyone associated with that soccer club. If this is a neighborhood club then the people in that club are likely to have similar incomes, and increasingly similar political alignment. The cookie on your machine identifies you as part of a group and an individual in that group. But it does not provide an identifier that can link you

to other transactions, domains, or credentials. You are provided a low quality anonymous identifier.

The value of identifying a person as a group member is that it enables targeted ads. By associating yourself with a group, you provide statistical information. The statistical information from the group enables more perfectly targeted advertisement and price discrimination.

Identity stands in for difficulty of physical credential reproduction in the digital realm. Digital anonymous credentials prove that this need not be the case. Identity also provides several secondary effects – a lack of privacy, more efficient marketing, a risk of identity theft, and the ability to reclaim your charge cards in a remote city using only the knowledge in your head.

Cryptography is the art of hiding information using mathematics. Therefore, while the slave's hair may have effectively hidden information, the use of mane instead of math places that particular technique outside the range of encryption. Cryptography can solve the problems of privacy and security simultaneously, while ensuring accountability.

Modern cryptography, using machines and codes too complex to break by even the most brilliant sleight of mind, was born in the turmoil before World War II. First the Italians stole the American substitution code, providing it to the Germans. This provided critical information even before the US entered the war, enabling the brilliance of at least one German general. Before Pearl Harbor, Colonel Bonner Frank Fellers, West Point Graduate and former personal assistant to MacArthur, provided detailed timely information to Washington about British plans. He was diligent from his post in Cairo to investigate every plan of the British Empire. By doing so he provided the information to Field Marshall Rommel as well. No doubt Rommel would have agreed with the post-war citation given to Fellers that noted, "His reports given to the War Department were models of clarity and accuracy." The historical record argues that the accurate information encrypted in weak American ciphers enabled at least one massacre of British forces. The War Department valued Fellers' clarity so much that they cleared his security practices in a review in June 1942 despite British complaints. Fellers was recalled in July of 1942, after the British provided decryptions of his reports to the surprised Americans. Thus on October 23 the 8th Army attack on the German positions led by the Dessert Fox came as a complete surprise. The fox had lost his seventh sense.

Later the tables turned with the well-known breaking of the German Enigma machine and the Japanese Purple code. Alan Turing is rightly famed for designing the first computer, which vastly sped the cracking of specific keys for the German Enigma machine. William and Elizabeth Friedman were the less known husband and wife team who decoded the Enigma-based machines used by the Japanese for their communications before and during World War II.

The ability to read Axis codes allowed the Allies to target and shoot down the plane of Admiral Isoroku Yamamoto 18 April 1943. Yamamoto