THE FILES FROM THE ORIGIN POINT

The information below is related to The Origin Point: A Future Tech Cyber Novella, the prequel to the Life Online Files book series by Case Lane. This document covers one issue discussed in the novella.

Below is the redacted summary from the Discrimination File.

DISCRIMINATION

Preventing the next Dr. King or Ms. Steinem from Gaining a Foothold: Hiding Race and Gender Bias in Website Code

THE ISSUE: *Businesses will be able to program race and gender discrimination into the software code of websites, preventing targeted groups from obtaining a product or service, or a fair price.*

Hanging a "Whites Only" sign outside of your business is likely to generate the wrath of civil rights groups, the immediate reaction of law enforcement flying the flag of the 14th amendment, and no end of taunting from local teenagers. The local Better Business Bureau will know to disown you, and what few patrons that remain will only gingerly offer support, usually behind the barrel of a shotgun. But if you code "Whites Only" into the software code of your business' website, you may be able to circumvent all of this unrest with no pushback.

The decision of Internet companies, retailers and other organizations to collect online personal data that can be used to create individual profiles, may lead to the creation of cyber Jim Crow for businesses that want to carefully manage their clientele. This not only applies to traditional bias along race and gender lines, but also discrimination by profession, zip code, education and every other factor that is being secretly collected by entities that consumers do not know.

Businesses are already in a position to readjust rates and prices based on selected factors. Creating another level of adjustment for the consumer's demographics would not be a difficult leap. A resort hotel trying to avoid journalists could code "no vacancy" when a user with that profession attempts to make a reservation. A business looking to encourage an affluent, youthful clientele could provide limited customer service when an undesirable age or zip code makes an inquiry. The question is – how would you avoid getting caught?

In the past, a person would try and rent an apartment, which is available when calling about it, and then rented as soon as the landlord sees the prospective tenant. The prospective tenant would send a different demographic friend to try the same approach, and document the results. In the cyber world, where data is updated second by second, consumers would find it difficult to prove that a "no vacancy" at a particular point in time was only directed at one user. Complainants would have to subpoena the offending code, and have the program deciphered to prove that it was set-up to avoid specific groups. Right after an allegation, a business could easily replace or re-program the code, removing any trace of suspect software. A consumer would have a difficult time conclusively detecting discrimination, and making a valid claim.

The real issue for consumers is that Internet companies have made these practices possible by collecting and distributing personal information, without transparent standards. This action, by itself, has opened the door for the future civil rights violators.

THE PROBABILITY: Easy to do and difficult to prove, the current competitive marketplace may only be delaying what businesses could determine is an acceptable risk.