United States privacy law follows a general pattern, particularly for internet and electronic data. The law identifies some type of record that raises privacy concerns, e.g., stored electronic communications (SCA) or electronically transmitted medical data (HIPAA). The law then requires information custodians to refrain from disclosing such information—or use safeguard to protect such information. This paradigm sees privacy as binary—either it is private or disclosed. United States law accepts this view, in general refusing to protect the privacy of information "shown to the public." And, many academics see the internet as reinforcing this view—once information gets out on the web, privacy is, it is commonly said, gone. This view of privacy is incomplete.

Privacy is contextual. For instance, most people do not want their co-workers to know their medical histories, but if there were an emergency and doctors and nurses needed that information, most people would not care whether a receptionist or ER bystander peeked at their records.

Privacy is idiosyncratic. Some people simply don't care about it. For instance, the journalist and author Jeff Jarvis campaigns against privacy and blogs about his impotence, incontinence, and other intimate details resulting from his bout with prostate cancer.

Privacy is relative. Consider a search incident to arrest of an individual with smartphone. The arresting officers are free to look into the individual's emails, social media, etc. But, if the individual passwords the phone, the officers will have to first crack the code. Depending on the state, they would have roughly 10-20 minutes to do so. All the privacy you need in that moment is a password protection system better than that which the officers have.

If privacy is highly contextual, idiosyncratic, and relative, then any one privacy rule or standard will inevitably over-include and under-include. The socially optimal policy, on the other hand, would allow individuals maximal freedom in determining their own privacy. Regulation should work to strengthen tools which give individuals choice in their privacy. These tools include anonymity/pseudonymity, encryption, using proxies for internet searching, etc. Even in the age of de-anonymization of PII, these tools can create noise in the computer programs designed to de-anonymize PII and thereby protect privacy.

More broadly, if privacy has both public and private good components, then individuals should "purchase" privacy—through the use of privacy tools—at a quantity equal to their preferences. Viewed in this manner, privacy becomes a cost function. When individuals face steep costs in controlling their information; regulation should mandate privacy or lower its cost allowing individuals to select levels of privacy they wish.

In the internet context, "code as law" emerges, as network engineering choices over internet and browser design dictate privacy options and the degree to which individuals can "purchase" privacy: privacy emerges as a system design question. Macro-level legal policy choices,

therefore, should be made to optimize choice in privacy, not dictate one standard. The legal loci for these system design question are often obscure and technical, *i.e.*, the information required by RIRs for domain registration, the use of pseudonymity in contracting for internet services, or government-mandates for computer protocols to identify online users. This paper aims to examine these too often ignored legal issues and the privacy trade-offs they present.