Privacy by Design (PbD) and Privacy Enhancing Technologies (PETS) as a practice seems to be very focused on the creation of security policy and law. While this way of viewing security has many advantages, because their is a clear void in modern policy and law as it relates to security, I think this approach has a major blind spot. Slight revisions to some of the underlying assumptions might help us formulate a more powerful approach, one that empowers the user. When I worked at Pandora, we empowered users to curate their own content, and as a result we noticed higher overall engagement. If we also empower groups to understand security for themselves we may be able to usher in a new era of security, a space where people are able to create security without total dictation from engineers and security professional.

The basic premise of most Privacy by Design (PbD) and Privacy Enhancing Technologies (PETS) is that “We the engineers and security professionals understand what needs to happen with your personal information, we can design a system that will protect what you think is important”

> Our knowledge of security as a practice helps us understand how to secure your information. **FALSE**. Knowledge is only a part of understanding. Understanding requires more than just facts, it also requires context. Experiential knowledge has more weight when approximating and reckoning the meaning of context. Most of the time we are simply designing security based on our best guess of the user’s context, which is implicitly biased. Furthermore, since it is impossible to predict the context of every user, we must empower the user to create security for themselves in the moment, rather than pretend that we can design all the security a user needs in any given moment or interaction.

> We need to tell people in the role of users how to secure themselves. **FALSE**. This might cut at the heart of our understanding of security. But I am going to speculate that if given the **proper** **disclosure** in the moment, people will make a security choice that is right for them. If systems were designed to ask for user what to do when security moments arose, I predict that people would make decisions to protect what is important to them. For example, when choosing a password, a simple prompt that tells the user their password is weak or strong ( this exists in many sites already ) and what to do to create a strong password is good security design because it educates and empowers the user.

I can appreciate the strides made to design secure systems, and create technology with powerful security defaults. However, the adversary we are facing in cybersecurity is not static. Rather than focus on designing a system that secures privacy by design, why not focus on a system that makes the actions of a system transparent by design? Privacy is defined by Westin as: “*the claim of individuals...to determine for themselves when, how and to what extent information about them is communicated to others.”*

Instead automating privacy, we should be automating disclosure and depending on the user for manual permissions.