Heather: The importance of protecting PII

Hello, my name is Heather and I'm the Vice President of Security Engineering at Google.
PII is everywhere.
It's a fundamental part of how we are all working online all the time.
If you are using online resources, you are probably putting your PII out there somewhere.
There's some of your PII that lots of people know, such as your name.
And then there's sensitive data that you don't want very many people to know, such as your bank account number or your private medical health information.
And so we make these distinctions often because this kind of information needs to be handled differently.
Everything that we do now, from school to voting, to registering our car happens online.
And because of that, it's so important that we have safety built-in by default into all of our systems.
Here's some tips.
You should always encrypt the data as much as you can when it's being stored at rest.
And secondly, when it's transitting over the Internet, we always want to encrypt it using TLS or SSL.
Third, within your company, you should think very clearly about who has access to that data.
It should be almost no one if it's very sensitive.
And in the rare cases where somebody does need to access that data, there should be a record of that access, who accessed it, and a justification as to why.
And you should have a program to look at the audit records for that data.
The most important thing to remember is if you have a situation where PII has been compromised, remember that's someone's personal information and your response wants to be grounded in that reality.
They need to be able to trust the infrastructure, the systems, the websites, the devices.
They need to be able to trust the experience they're having.
For me, that's the mission: To help keep billions of people safe online every day.

Revision #2
Created 2023-07-20 17:23:03 UTC by naruzkurai
Updated 2023-08-15 18:44:11 UTC by naruzkurai