My name is Karlen Burris. I managed independent 3rd party cell phone repair shops for 10 years and now work at an R2 2013 certified electronics recycling facility. 3rd party repair improves and empowers citizens in all communities by giving them varied and affordable alternative to insurance based repairs and a place to trust for consultations in matters related to device implementation, data and security. The ability to repair has taken the community far and the right to repair will stretch that ability even farther for all technicians and the communities they serve, in a safer and more responsible fashion.

The statement “right to repair improves cybersecurity” I perceive as true, with two points in particular. Access to schematics and service manuals should curb the need of technicians to circumvent domestic IP law and leave customers data, and their own, open to vulnerabilities when they must turn to black market solutions. An example is a usb thumb stick that has schematics and solutions for current flagship models. It is a subscription based service that runs off of Chinese servers, with no guarantee they are not leaving the target computer open to compromise. Without these solutions, many repairs are not possible. Shops and consumers must weigh these risks against purchasing new products or losing data. Another instance of security, the passing of the right to repair can put an added level of trust and skill to your local vendor and break the cycle detailed below. The example is with a device with a latent defect that would inevitably lead to failure, dropped or not.

1. A new device is set up with all of a consumers relevant information (banking, health kit, photo, contacts, etc.). But no backup plan for data is implemented.

2. Phone is dropped and results in a shifted/broken capacitor causing a short to ground (it appears to draw no power and will not turn on) The device is just outside of the 1 year manufacturer warranty, so a replacement device is already out of the question, but the data is what is needed in this case.

3. Device is taken into 3rd party shop, a new battery is tested and does not turn the phone back on. Testing a new battery is often the most common and only way a shop has to diagnose a problem with this open ended nature. (This is where the cycle can be broken with access to solutions and schematics. Until then, the cycle usually continues as below.)

4. Phone and data is listed unrecoverable (access to schematics and solutions would point out an avenue to bring device back to working order and recover data)

5. Phone sits in junk drawer until it is recycled (properly or improperly)

6. Data is now lost and floating. Even is device is eventually restored to working order, account locks and passwords cannot be recovered now that is removed from the original owner, phone is now broken down for parts if possible or potentially waiting to be compromised and have the data pulled from it through nefarious means.