Technical Disclosure Commons

Defensive Publications Series

March 29, 2017

Anonymous mobile device connections

Titus E. Davis
Hewlett Packard Enterprise

Anonymous mobile device connections

This disclosure relates to the field of mobile device communication. This idea enables anonymous connections through the use of sound, lights, or images that connect individuals or groups without any identifying information.

Despite the vast use of social media on mobile devices there is not a good way to make connections without the use of identifying information. The idea is to use sound, light, or images to make connections between individuals or groups without the need to exchange phone numbers, email address, links, tags or any identifying information. This technology can be used even if the individuals or groups are not in direct contact with each other.

A typical problem with organizing an event such as a school field trip is the exchange of identifying information to link the mobile devices of the parent volunteers who are helping with the trip. No one really wants to give out phone numbers, email addresses or social media links to strangers that will only be used for a few hours.

Another example is standing in line for an event such as a concert, and you meet new people that you would like to communicate with after the concert. Again, you don’t want to exchange phone numbers, email address, social media pages or anything identifying to people you don’t know.

What if you see someone at a distance that you want to connect with and cannot easily reach them to exchange a phone number or email address?

How is this accomplished?

Each user or device will have to create an account with contact information that will only be used by the supporting servers and accessible by the account holder. The servers holding the account information for this technology will need to be accessible by the mobile devices over a network or cell link. The servers would maintain filters for age appropriate groups and maintain logs of all connections that may be required for law enforcement. This is no different than users of email or social media pages today. Each participant of this technology will need to use a dedicated application or an existing application with this technology integrated within it. Ideally this technology will be integrated into existing social media and business applications.

Once the application is running on the mobile devices and a connection is available to the account servers the users or a group of users are ready to make anonymous connections. In the simple case of using images the originating mobile device will contact the servers for a QR code or another unique image and display it on the screen. The receiving devices will contact the servers and indicated that they are ready to view the image using the camera on the device. The servers make the connections between the devices using the unique image. Once the connections have been made communication in any form the devices support (text, video, audio) will be available. At any time, users can drop out of the connection. They can only reconnect if they have access to the original image.

For longer distances or larger groups a unique sound would be generated by the originating device so the servers can find and link the receiving devices. The use of sound to make the connection would enable the use of a public-address system to link a large group even if they were not in the same place.

For even longer distances, larger groups, or places where the ambient sound is high, the devices camera flash or screen could be used to send the linking token using light pulses.

In all cases only the application servers know the connection endpoints and manage the traffic. Phone calls, video calls, text, instant messaging, and email could be passed through the servers protecting the identity of the endpoints. This technology solves the problem of connecting users or groups of users without exchanging personal information. The connections are persistent until closed by the users. For ease of use the connections will be named by the users to facilitate the handling of multiple instances.

The life of an anonymous connection assuming all devices have this technology enabled, and have internet access:

- Originator opens the application and requests a new connection.
- The supporting servers create a unique token to be shared and sends to originating device.
- Originator selects the devices screen, flash, or speaker for the token transport method. The device locally creates the image, sound, or light sequence based on the token and transport method selected.
- Receivers open the application and select “wait for token” while pointing the camera or microphone toward originator. The receiving devices opens the microphone and camera if equipped and waits for the token.
- The receiving device decodes the transported token and sends to the supporting servers. The servers match originator with the receivers and creates the links.
- The users name the connection for ease of use and to identify the event.
- Any call, text, email, video, send to the named connection will be transported through the servers protecting the identity of the end points. The users only see the named connection as the identifier.
- Example: User places a call to the named connection, the servers lookup the real phone numbers of the participants of this connection using the stored account information and places calls with a generic caller ID. The participants will see a call from the named connection with a generic caller ID. None of the connection participants will see a real phone number or anything identifying the source other than the name of the connection. The same for email or text messages, they would be transported through the servers with only the connection name as the identifier. All members of the named connection would be included.
- At any time users can close their end of the connection and the servers will remove the devices link.

Recurring group calls are now easy as any user calling the named connection rings all of the phones. At the end of a lecture the speaker can easily send the slides to the participants without the need for email address, share points, or web sites, greatly simplifying distribution. If the connection was left open then updates and speaking schedules could be easily distributed to the group.

An application like Skype could easily use this technology as it already has the ability to place calls, video calls, instant messaging, and email. Integrating this technology would enable anonymous connections to individuals or groups meeting the needs of a large demographic.

Disclosed by Titus E Davis, Hewlett Packard Enterprise