Consider example you have a application like this –

Now you added some xyz script in your application, which is from other source all together or probably you have added some IFrame in such cases and that is again from some 3rd party IFrame so this is cross domain iframe, so inside your webpage you have all of these things then what the chances are? The chances are this xyz script or iframe any of these things can steal or get the access from the browser on behalf of you and your user will never get to know ohh you ask for the geo location or who taking the access of the mike or who taking the access of the video.

So someone have to take care of, there are certain headers there are certain policies that can help you to safeguard that, example

app.use((req, res, next) => {

  res.setHeader('Permissions-Policy', 'geolocation=()');

  next();

})

Because of this above middleware the app cannot access the geo location,

Refer pdf for more info.