FTC PrivacyCon
January 14, 2016
Segment 5
Transcript

>> SO WE CAN STAY ON SCHEDULE,

WE'RE A FEW MINUTES BEHIND.

>> ALL RIGHT OUR LAST PANEL OF

THE DAY WILL LOOK AT ISSUES

AROUND SECURITY AND USABILITY AS

IT RELATES TO PRIVACY.

I'D LIKE TO WELCOME OUR FIRST

PRESENTER, SARTHAK GROVER, HE IS

A PH.D. STUDENT AT PRINCETON.

>> HI EVERYONE, I'M SARTHAK AND

I'LL BE PRESENTING A WORK ON THE

INTERNET OF UNPATCHED THINGS.

THE CURRENT STATE OF DEVICES WE

BASICALLY ENDED UP STUDYING

NETWORK TRAFFIC FROM A BUNCH OF

SMART TWICES THAT ARE REALLY

POPULAR AND WE WANT TO TALK

ABOUT HOW THESE DEVICES MIGHT

POTENTIALLY LEAK INFORMATION.

MY DIRECTION IS TO ENCOURAGE YOU

TO THINK OF POLICIES THAT CAN

STOP THIS LEAK OF INFORMATION.

HOW IS THE SMARTPHONE OR THE IOD

ENVIRONMENT VERY DIFFERENT FROM

THE CONVENTIONAL MOBILE OR

COMPUTER ENVIRONMENT?

THE PROBLEM WE'RE HERE IS WE

HAVE A LOT OF MANUFACTURERS AND

WE HAVE SMALL STARTUPS COMING

WITH THEIR OWN DEVICES, THEY MAY

BE HIDING NOVICE PROGRAMMERS.

APART FROM THAT THESE DEVICES

HAVE LOW MEMORIES, THEY MAY NOT

HAVE CAPABLE HARDWARE TO ENFORCE

SECURITY PROTOCOLS WHICH WE USE

IN COMPUTERS AND PHONES.

THIS MAKES IT PRETTY DIFFICULT

TO FIRST OF ALL IMPLEMENT

SECURITY PROTOCOLS ON THESE

DEVICES BUT APART FROM THAT A

BIGGER ISSUE IS THAT THE CURRENT

SMARTPHONE MODEL WORKS LIKE

THIS.

YOUR DEVICES INSIDE THE HOME

SEND ALL THEIR INFORMATION TO
THE CLOUD TO A PARTICULAR
SERVER.
IN FACT IF YOU HAVE TWO DEVICES
IN THE HOME AND THEY WANT TO
TALK TO EACH OTHER, CURRENTLY
THEY WILL TALK TO THE CLOUD AND
THE INFORMATION WILL GET BACK TO
THE HOME AND YOU KNOW SOMETHING
WILL HAPPEN IN THE HOME THEN.
SO WHAT WE HAVE OVER HERE IS A
PRETTY BAD COMBINATION.
YOU HAVE HARDWARE WHICH IS
INCAPABLE AND INFORMATION WHICH
IS ALWAYS BEING SENT TO THE
CLOUD.
SO THIS COMBINATION RESULTS IN
POTENTIAL PRIVACY PROBLEMS.
SO NOW, IOD DEVICES WHICH IS
SENDING NETWORK TRAFFIC WITHOUT
SECURITY PROTOCOLS MAY END UP
LEAKING SOME INFORMATION ABOUT
THE USER, THEY MAY END UP

LEAKING INFORMATION ABOUT WHAT
DEVICE IS BEING USED INSIDE THE
HOME AND THEY MAY ALSO END UP
LEAKING INFORMATION ABOUT
WHETHER THE USER IS HOME OR WHAT
HE'S CURRENTLY UP TO.

ANYONE SETTING ON YOUR NETWORK
PATH MAY FIND OUT WHAT YOU ARE
CURRENTLY DOING INSIDE YOUR HOME
AND THIS IS A BIG FAULT.

SO WHAT OUR AIM IS RIGHT NOW IS
TO BASICALLY TAKE UP A FEW
DEVICES IN OUR CASE STUDY AND
STUDY WHAT KIND OF PERSONAL
INFORMATION OR USER ACTIVITY
INFORMATION THEY LEAK TO THE
CLOUD.

SO WHAT WE DID WAS, WE BASICALLY
BOUGHT SOME POPULAR DEVICES.

WE WENT TO AMAZON.COM, WE
SEARCHED FOR POPULAR HOME
NETWORK DEVICES AND WE ORDERED
THEM.

WHAT I'M GOING TO SHOW YOU IS
RESULTS FOR NETWORK TRAFFIC
ANALYSIS FOR FIVE DEVICES A
CAMERA A PHOTO FRAME A HUB AN
UBI SMART SPEAKER AND A NEST
THERMOSTAT.
WHAT WE'RE INTERESTIN RIGHT NOW
IS WHAT KIND OF INFORMATION
THESE COMMON DEVICES LEAK TO THE
NETWORK.
AND THE FIRST DEVICE I PICK UP
IS THE DIGITAL PHOTO FRAME BY
PICSTAR.
AWAY WE FOUNDING IS ALL TRAFFIC
SENT BY THIS DEVICE IS SENT IN
UNENCRYPTED FORM.
IT'S DOWNLOADING DEVICES IN THE
CLEAR AND ALSO WHAT ACTION YOU
TAKE ON THIS DEVICE, FOR EXAMPLE
YOU PRESS A BUTTON SAY YOU PRESS
THE PLAY RADIO BUTTON THAT WILL
GO IN A CLEAR SJD PACKET WHICH
SOMEBODY ON THE NETWORK CAN

READ, IF SOMEBODY IS SITTING

OUTSIDE IN THE NETWORK LIKE ISP

OR A MALICIOUS PASSIVE LISTENER

CAN SEE WHAT YOU'RE DOING

THROUGH THE PHOTO FRAME.

APART FROM THAT IT IS ALSO

CAPABLE OF DOWNLOADING RADIO

STREAMS AGAIN IN THE CLEAR.

AND EXAMPLE OF WHAT KIND OF

INFORMATION WE SEE, THESE ARE

SNAPSHOTS FROM WIRESHOCK

BASICALLY AND WHAT WE SAW WAS

THAT YOUR E-MAIL WHICH YOU

CONFIGURED YOUR ACCOUNT WITH, IS

POTENTIALLY LEAKING DATA.

9 ON THE NETWORK PART CAN

ACTUALLY HAVE A LOOK AT THIS

E-MAIL.

IF YOU PRESS THE LIST CONTACTS

BUTTON OR THE RADIO BUTTON,

ANYBODY TON NETWORK CAN HAVE A

LOOK AT WHAT YOU JUST PRESSED.

SOMEBODY ON THE ISP SAYS, THIS

PERSON IS LISTENING TO THE RADIO
FROM THE PHOTO FRAME.
I DON'T KNOW WHY YOU WOULD
LISTEN TO THE RADIO FROM THE
PHOTO FRAME BUT -- BASICALLY
WHAT I SAY IS YOU CAN LISTEN TO
THE ACTIVITY, JUST BY ROOK AT
THE NETWORK INFORMATION.
THE SECOND DEVICE WE PICKED UP
WAS A SHOCK SECURITY CAMERA.
IT'S A PRETTY COMMON CAMERA
WHICH IS USED FOR SECURITY
MONITORING IN HOMES.
IT HAS LIKE MOTION DETECTION.
WHAT WE SAW WAS THAT ALL THE
TRAFFIC AGAIN WAS BEING SENT IN
CLEAR TEXT.
NOW, THIS SECURITY CAMERA
ACTUALLY REQUIRES A LOG IN.
IF YOU WANT TO REVIEW THE STREAM
YOU'RE SUPPOSED TO ENTER A
PASSWORD, THAT DOESN'T MEAN THE
STREAM IS HE BE CRYPTED.

ANYBODY CAN LOOK AT WHERE THE
STREAM IS AND WHAT IS IN THE
STREAM.
IF YOU PRESS A BUTTON WHATEVER
YOU DID WILL I STILL GO TO AN
SGP GET PACT AGAIN UNENCRYPTED.
RADIOS ARE BEING SENT AS JPEG
FRAMES.
IF YOU PRESS THE FTP BUTTON ALL
YOUR DATA IS BEING UPLOADED IN
THE CLEAR.
THIS IS AN EXAMPLE OF WHAT THESE
THINGS LOOK LIKE.
FTP IS USING RANDOM PORTS YOU
CAN'T RELY ON THE NETWORK TO
SECURE YOU AGAIN BECAUSE THESE
ARE NONSTANDARD PORTS WHICH ARE
BEING USED BY THE DEVICE.
THIS IS BASICALLY PRIVATE DATA
WHICH IS BEING UPLOADED.
THE THIRD DEVICE WE ENDED UP
LOOKING AT WAS THE UBI.
SO THIS IS LIKE I THINK IS A

PRECURSOR OF THE AMAZON ECHO,
THIS IS A SMALL VOICE BOX WHICH
YOU CAN TALK TO, INTERFACE WITH
OTHER DEVICES.
WE HAD THIS WITH THE NEST.
ALL VOICE TO TEXT FIRST OF ALL
ALL VOICE YOU TALK TO THE UBI
WILL GET CONVERTED TO TEXT ON
THE DEVICE ITSELF AND THEN TEXT
IS SENT IN CLEAR AGAIN TO A
SERVER OUTSIDE.
THE SERVER HERE WAS THE UBI.COM.
APART FROM THAT THE UBI ALSO HAS
CERTAIN SENSORS, FOR EXAMPLE
LIGHT SENSORS AND TEMPERATURE
SENSORS WHICH ARE STILL SENDING
THEIR READINGS IN THE CLEAR.
AND THE INTERESTING THING OVER
HERE IS WHEN WE INTERFACE THIS
DEVICE WITH THE NEST IT USED
ENCRYPTION AND SPOKE OVER SGTPS
BUT WHETHER IT WAS TALKING TO
ITS OWN SERVER IT WAS USING SGP

AND CLEARLY THIS DEVICE HAS THE
CAPABLE OF ENFORCING SECURITY.
BUT SOMEHOW THE POLICY WHATEVER
POLICY THEY CAME UP WITH THEY
DID NOT ENFORCE ENCRYPTION, ONLY
WHEN THEY ARE TALKING TO THE
GOOGLE API THEY ENFORCE THIS
ENCRYPTION.
THIS IS AN EXAMPLE THAT SHOWS
HOW SENSOR READINGS WHICH ARE
AVAILABLE.
THESE SENSOR READINGS CAN LEAK
INFORMATION ABOUT WHETHER OR NOT
SOMEONE IS ON THE PATH OR NOT,
TO KNOW WHETHER THERE'S A USER
STHIED THE ROOM OR NOT BASED ON
THE LUMINOSITY VALUE.
FURTHERMORE, LIKE WHEN WE WERE
CHATTING WITH THE DEVICE ALL THE
TEXT WAS CONVERTED TO CLEAR TEXT
AND THEN SENT TO THE NETWORK.
HERE YOU CAN SEE AN EXAMPLE WHAT
THE CHATS LOOKED LIKE WHEN I

MONITORED THEM ON THE LAPTOP

GATEWAY.

THE NEXT DEVICE WE LOOKED AT WAS

THE NEST THERMOSTAT.

NOW WE'RE ACTUALLY COMING TO THE

MORE SECURE DEVICES AND THE BIG

ONES TOO.

THE NEST THERM AT THAT TIME FROM

GOOGLE ACTUALLY WAS PRETTY

SECURE.

ALL INFORMATION WAS USING

ENCRYPTION AND HGTPS.

WHAT WE ALSO FOUND OUT WAS SOME

OF THE UPSTAIRS IN COMING WERE

IN THE CLEAR AND WE WERE NOT

SURE WHY, SO WE CONTACTED NEST

ABOUT THIS, TURNED OUT IT WAS A

BUG AND THEY FIXED IT.

SO HERE IS AN EXAMPLE OF WHAT WE

FOUND INITIALLY.

OUTGOING TRAFFIC WAS SECURE, BUT

CERTAIN INCOMING CONTACTS WERE

NOT SECURE.

WE TO THE NEST ABOUT IT, THEY

THANKED US AND THEY FIXED IT.

THE LAST DEVICE WHICH I'M GOING

TO TALK ABOUT IS THE SMART

THINGS HUB, BY SAMSUNG.

PRETTY POPULAR HUB FROM A PRETTY

BIG COMPANY.

THE GOOD THING WAS ALMOST ALL

THE TRAFFIC COMING OUT OF THIS

DEVICE OR GOING INTO THE DEVICE

WAS TOTALLY SECURE OVER DLS,

THERE WAS NO FLOW AT ALL THE

FLOW WAS TO AN AMAZON NATIVE IN

EACH INSTANCE.

BUT THE INTERESTING THING EVEN

THOUGH THIS DEVICE IS IN ITSELF

SECURE IN FACT I SEE THIS AS THE

MODEL OF FUTURE IOD DEVICES

WHICH ARE COMPLETELY SECURE,

THERE IS STILL BACKGROUND

INFORMATION LIKE THREE OR FOUR

PACKETS, GOING TO

SMARTTHINGS.COM WHICH CAN

SOMEHOW LET YOU FINGER PRINT THE DEVICE.

THE SMART THING IS A HUB, WHICH MEANS BASICALLY YOU HAVE OTHER THINGS ATTACHED TO SMART THINGS OVER OTHER PROTOCOLS AND YOU DON'T HAVE A DIRECT VIEW OF THE SENSOR.

SO SMART THINGS ITSELF MAKING ALL OF THE INFORMATION COMING OUT OF THE HOUSE SECURE AND THEN SENDS IT OUT.

BUT A PERSON SITTING AT THE ISP LEVEL CAN STILL FIND OUT YOU HAVE A SMART THINGS HUB INSIDE THE HOME.

SO THIS BRINGS US TO MY CONCLUSION AND SOME IMPLICATIONS ON THE POLICY.

BASICALLY, I DON'T WANT TO SOUND PESSIMISTIC OR DRAMATIC BUT THAT'S WHAT THE HEADING IS, BE AFRAID.

WE KNOW HOW TO ENFORCE SECURITY
DEVICES ON HAND HELD DEVICES.
THERE ARE A LOT OF LONG TALES OF
SMALL ONCE, IT'S DIFFICULT TO
ENSURE THAT THEY ALL FOLLOW THE
SAME STANDARD.
THESE DEVICES ARE ALSO SOMETIMES
VERY LOW CAPABILITY.
THEY DON'T HAVE A WAY TO
IMPLEMENT DLS ON THE PACKETS
THEY ARE SENDING OUT AND THEY
END UP USING NONSTANDARD PORTS
AND PROTOCOLS.
THE GOOD NEWS IS WE ARE TRYING
TO MAKE AN EVIDENT.
FOR EXAMPLE I FOUND THIS HANDOUT
ON THE OUTSIDE, REGARDING
BUILDING THE INTERNET OF THINGS.
MAYBE THE NEW DEVICES WHICH COME
UP WILL HAVE SECURITY INHERENT
IN THEM.
THE SECOND THING IS OKAY, SO
WE'VE FIXED DEVICES WHICH ARE

COMING UP NOW.

WHAT ABOUT DEVICES WHICH ARE

ALREADY PRESENT?

HOW DO WE GET PEOPLE TO PATCH

THEM UP OR FIX THEM?

SO FIRST OF ALL WE WANT TO

ENCOURAGE PEOPLE TO LOOK FOR BUG

AND ONE WAY WOULD BE BUG

BOUNTIES, BUG BOUNTIES MAY WORK

FOR THE BIG GUISE BUT THE IODOD

DOMAIN HAVE A LOT OF SMALL

MANUFACTURERS COMING UP AND WE

DON'T KNOW IF BUG BOUNTIES WILL

WORK FOR THAT AND WHETHER THE

DEVICE WILL BE POPULAR ENOUGH TO

HAVE DEVICES TO LOOK FOR

VULNERABILITIES IN THEM.

HOW DO WE ENFORCE SUCH KIND OF

THINGS?

WHO IS RESPONSIBLE?

WILL THE GOVERNMENT TRY TO

ENFORCE BUG BOUNTY PROGRAMS, OR

THE MANUFACTURER, IF YOU FIND

BUG WE'LL GIVE YOU MONEY, AND
WHO IS RESPONSIBLE FOR THE
UPDATING PART?
IF THIS IS USING YOUR NETWORK IS
THE USER RESPONSIBLE FOR
ANYTHING WHICH GOES WRONG OR THE
ISP OR IS IT THE MANUFACTURERS?
I WANT TO END WITH LIKE SOME OF
THE WORK WHICH WE'RE CURRENTLY
UP TO RIGHT NOW.
WE'VE TALKED ABOUT HOW WE CAN
IMPROVE FUTURE DEVICES IN TERMS
OF THEIR SECURITY AND PRIVACY
POLICIES.
WE'VE TALKED ABOUT HOW WE CAN
IMPROVE CURRENT DEVICES BY
TRYING THE FIND BUGS IN THEM AND
VULNERABILITIES IN THEM.
THE APPROACH WE ARE TAKING RIGHT
NOW IS HOW TO IMPROVE SECURITY
AROUND PRIVACY POLICY ON THE
NETWORK.
BASICALLY, WE'RE TRYING TO

OFFLOAD POLICY TO THE NETWORK
LAYER.
FOR EXAMPLE, IN CASE OF A SMART
HOME ALL OF OUR INFORMATION IS
GOING TO GO THROUGH A GATEWAY
WHICH IS INSIDE THE HOUSE.
THIS GATEWAY MAY BE PROVIDED TO
US BY THE ISP OR MAYBE ON ITS
OWN.
MAYBE THERE ARE SECURITY DEVICES
WHICH WE CAN IMPLEMENT AT THE
GATEWAY ITSELF.
MAYBE WE CAN TET THE GATEWAY TO
ENFORCE STANDARDS, AT THE VERY
LEAST OUR GATEWAY COULD INFORM
OUR USER THAT HEY THERE IS
SOMETHING WRONG WITH YOUR
DEVICES OR THIS DEVICE IS NOT
USING THE RIGHT SECURITY
STANDARDS.
SO WHAT WE'RE LOOKING AT
CURRENTLY IS CAN WE OFFLOAD
DEVICE SECURITY TO A GATEWAY OR

THE NETWORK LAYER AND SECONDLY

HOW MUCH INFORMATION ABOUT THE

USER BEHAVIOR IS ACTUALLY LEAKED

TO OUTSIDE THE HOME NETWORK?

ALL RIGHT, THANK YOU.

[APPLAUSE]

>> THANK YOU.

NEXT WE WILL HAVE PROFESSOR

VITALY FROM CORNELL UNIVERSITY

AND CORNELL TECH.

>> THAT'S MY CLICKER, RIGHT?

>> YES.

>> HI.

THAT'S MY MIC?

HEY.

SO I'M VITALY.

AND I'LL BE TALKING ABOUT MOBILE

ADVERTISING TODAY.

SO MOBILE ADVERTISING IS PRETTY

BIG THESE DAYS.

IF YOU LOOK AT MODERN APP STORES

YOU FIND THAT A SIGNIFICANT

FRACTION OF APPS ARE FREE TO THE

USER.

AND THE WAY THEY MAKE THEIR

MONEY IS BY INCORPORATING

ADVERTISING.

SO IT SEEMS LIKE A VERY

REASONABLE QUESTION TO ASK, WHAT

INFORMATION ABOUT THE USER IS

ACTUALLY AVAILABLE TO

ADVERTISERS, THAT IS IF AN

ADVERTISER SUBMITS AN AD TO

MOBILE ADVERTISERS AND AN AD

DUETS SHOWN ON A USER'S PHONE

WHAT CAN THE ADVERTISER FIND OUT

ABOUT THE USER OF THE PHONE IN

WHICH THE AD IS BEING SHOWN?

THAT IS AN INTERESTING QUESTION,

APPARENTLY SO FAR THERE HASN'T

BEEN A GOOD ANSWER, VERY FEW

PEOPLE INVESTIGATED THIS SO THIS

IS WHAT WE DECIDED TO

INVESTIGATE IN THIS PROJECT TO

LOOK AT THIS.

BUT IN ORDER TO UNDERSTAND THIS,

WE FIRST NEED TO UNDERSTAND HOW

MOBILE ADVERTISING ACTUALLY

WORKS.

FROM A SOFTER PERSPECTIVE.

SO IT REQUIRES A LITTLE BIT OF

REVERSE ENGINEERING OF HOW

MOBILE SOFTWARE THAT ACTUALLY

SHOWS APPS TO USERS, HOW IT

ACTUALLY WORKS.

IT'S A LITTLE BIT SIMILAR TO

MOBILE -- SORRY TO MOBILE

ADVERTISING IS A LITTLE BIT

SIMILAR TO WEB ADVERTISING WITH

ONE CRUCIAL DIFFERENCE.

IN WEB ADVERTISING YOU TYPICALLY

HAVE A WEB BROWSER AND THE WEB

BROWSER IS JUST SHOWING AN APP.

WE'VE HAD A LOT OF TALKS AND

CONVERSATION ABOUT WEB

ADVERTISING.

IN MOBILE ADVERTISING THINGS ARE

A LITTLE DIFFERENT BECAUSE THERE

IS SOMETHING IN THE MIDDLE.

NAMELY, THERE IS AN APP LIBRARY.
THE WAY MOBILE ADVERTISING
WORKS, APPS THAT ARE SUPPORTED
BY MOBILE ADVERTISING IS
SUPPORTED BY APP LIBRARIES,
INCORPORATING MULTIPLE
LIBRARIES, BECAUSE THEY MAKE
MORE MONEY THAT WAY.
BETWEEN A THIRD AND HALF OF ALL
APPS THAT ARE AD SUPPORTED,
BEING USED TO SHOW APPS TO
USERS.
SO THE QUESTION I'M ASKING JUST
TO REPEAT IT, WHAT DO THESE ADS
THAT ARE BEING SHOWN INSIDE THE
MOBILE ADVERTISING LIBRARIES
WHAT DO THEY ACTUALLY KNOW ABOUT
THE USER OR WHAT THEY CAN FIND
OUT?
IN ORDER TO DO THIS WE NEED TO
LOOK AT THE STRUCTURE OF THIS
WHOLE ECOSYSTEM AND I PROMISE
I'LL TRY TO MAKE IT AS PAINLESS

AS POSSIBLE.

ALTHOUGH INVESTIGATING IT WAS

FAIRLY PAINFUL AND INVOLVED A

SIGNIFICANT AMOUNT OF REVERSE

ENGINEERING BUT IT ROUGHLY LOOKS

SOMETHING LIKE THIS.

THERE ARE THREE KIND OF BIG

PARTIES IN THE PICTURE, THERE IS

THAT APP WHICH IS BEING SHOWN ON

THE PHONE.

THERE IS THE ADVERTISING SERVICE

WHICH IS SUPPLYING ADS TO THE

PHONE AND THEN THERE IS THE

ADVERTISER WHOSE ADS ARE BEING

SHOWN.

AND THERE HAS BEEN A LOT OF WORK

PREVIOUSLY ON TRYING TO

UNDERSTAND WHAT INFORMATION IS

AVAILABLE TO THE ADVERTISING

SERVICE.BUT INSTEAD WE ARE

LOOKING AT WHAT IS ACTUALLY

AVAILABLE TO THE ADVERTISER.

AND IT IS NOT THE SAME QUESTION

BECAUSE THERE IS A BIG
DIFFERENCE BETWEEN THE
ADVERTISING SERVICE AND THE
ADVERTISER.
THE ADVERTISING SERVICE IS
TYPICALLY REASONABLY R RESPECTABLE
COMPANY THAT IS OWNED BY GOOGLE
OR TWITTER, THEY HAVE A
REPUTATION AT STAKE AND THEY
MAKE A LOT OF REVENUE.
WHEREAS ADVERTISERS WHICH IS
PEOPLE THAT SUPPLY THESE ADS
THAT ARE BEING SHOWN WHO KNOWS
WHO THEY ARE?
THIS IS DYNAMICALLY DETERMINED
THEY ARE IN REAL TIME SHOWN BY
AUCTION SYNDICATION ALL
DIFFERENT WAYS, NOT NECESSARILY
TRUSTED, HARD TO DETERMINE WHAT
INFORMATION THEY'RE TRYING TO
EXTRACT AND THAT'S WHY MOBILE
ADVERTISING LIBRARIES THEY GO TO
FAIRLY SIGNIFICANT LENGTHS TO

PROTECT USERS FROM MALICIOUS
ADVERTISING AND FROM SNOOP
ADVERTISING AND FROM ADVERTISING
THAT TETLY TRIES TO EXTRACT --
THAT STEALTHILY TRIES TO EXTRACT
INFORMATION FROM USERS.
I'M NOT GOING TO GO INTO THIS,
YOU CAN READ OUR PAPER IF YOU
WANT TO FIND OUT MORE ABOUT
THIS.
THE SHORT SUMMARY IS WHAT THEY
TRY TO DO IS TO SHOW EVERY AD
THAT THEY SHOW TO THE USER
INSIDE A LITTLE BROWSER
INSTANCE.
SO IT IS AS IF THERE'S A LITTLE
WEB BROWSER INSIDE EVERY
ADVERTISING LIBRARY AND THEY
SHOW AN AD INSIDE THAT THING.
AND THE GOOD NEWS ABOUT IT IS,
THEY CAN EFFECTIVELY RELY ON
SECURED AND PRIVACY PROTECTIONS
INSIDE WEB BROWSERS TO PROTECT

PHONE USERS FROM MALICIOUS

ADVERTISING.

SO TECHNICALLY THIS IS KNOWN AS

SAME ORIGIN POLICY BUT YOU CAN

THINK OF IT AS A WAY OF SAND

BOXING URCH TRUSTED ADVERTISING

TO MAKE SURE IT DOESN'T HAVE ANY

ACCESS TO THE PHONE AND CAN'T

LEARN ANYTHING IT SHOULDN'T

LEARN FROM THE PHONE.

AND MOSTLY IT WORKS WITH ONE

LITTLE EXCEPTION.

MOBILE ADS THESE DAYS NEED

ACCESS TO WHAT AN ANDROID PHONE

IS KNOWN AS EXTERNAL STORAGE.

AND THERE ISN'T A NEED TO DO

THIS, IT'S TO -- FOR REACH MEDIA

BECAUSE PEOPLE WHO VIEW

ADVERTISING AND ESPECIALLY

PEOPLE WHO SUPPLY THIS

ADVERTISING THEY WANT TO REACH

EXPERIENCES, THEY WANT VIDEO

THEY WANT IMAGES AND BECAUSE OF

THAT THEY NEED TO CACHE A LOT OF

INFORMATION ON THE DEVICE SO

THEY HAVE ACCESS TO EXTERNAL

STORAGE.

TO BE SAFE THEY ALLOW ADS TO

LOAD INFORMATION -- SORRY IT

CANNOT READ IT, IT CAN JUST LOAD

IT AND SHOW IT TO THE USER

WITHOUT BEING ABLE TO READ IT.

SO THAT LOOKS FAIRLY HARMLESS.

EXCEPT THAT ANDROID EXTERNAL

STORAGE IS KIND OF THIS WEIRD

THING.

IN ANDROID EXTERNAL STORAGE

THERE IS REALLY NOT A WHOLE LOT

IN THE WAY OF ACCESS CONTROL

PROTECTION IS.

THAT IS, IF THERE ARE MULTIPLE

APPS RUNNING ON THE DEVICE AND

THEY STORE EXTERNAL INFORMATION

ON EXTERNAL STORAGE, THIS SHOULD

NOT IMPLY A LOT ABOUT SECURED

INFORMATION ABOUT MOBILE ADS, AS

I TELL YOU MOBILE ADS CANNOT
ACTUALLY READ EXTERNAL STORAGE,
THEY CAN TRY TO LOAD THEM AND
SLOW THEM TO THE USER BUT THEY
CANNOT GET ACCESS TO THEM
DIRECTLY, THEY CANNOT LOOK AT
THEIR CONTENT.
SO FAR SO GOOD.
I KEEP TALKING ABOUT THIS ONE
LITTLE WEIRD THING.
THEY CANNOT READ THEM BUT THEY
CAN TRY TO LOAD THEM.
WHY IS THIS INTERESTING?
IT TURNS OUT, THAT BY TRYING TO
LOAD A FILE THAT DOESN'T BELONG
TO THEM, MOBILE ADS CAN LEARN A
LITTLE BIT, THEY CAN LEARN
LITERALLY ONE BIT OF
INFORMATION.
THEY LEARN IF A PARTICULAR FILE
EXISTS ON THE DEVICE OR NOT.
THEY CANNOT READ IT.
THEY JUST LEARN IF A FILE WITH A

PARTICULAR NAME EXISTS.

THAT SEEMS LIKE OKAY, ALL RIGHT,

THAT'S FASCINATING WHY AM I

TALKING ABOUT THIS?

THAT'S REALLY A VERY SMALL

AMOUNT OF INFORMATION.

SO NOW LET'S LOOK AT HOW THIS

INFORMATION PLAY BE USED BY A

MOBILE APP.

LET'S LOOK AT THIS INFORMATION,

NOTHING TO DO WITH MOBILE

ADVERTISING, GOOGLE PLAY STORE

THAT HAPPENS TO BE A DRUG

SHOPPING APPLICATION, HELPS A

PERSON TO LOOK AT A PHARMACY, IF

SOMEONE IS TAKING A PARTICULAR

MEDICATION, THEY CAN LOOK AT A

PHARMACY NEARBY WHERE THE DRUG

IS LOWER.

THE FACULTY THAT A PERSON IS

TAKING ONE OF THESE MIGHT BE

CONSIDERED SENSITIVE BECAUSE

THIS HAS TO DO WITH ANXIETY AND

VARIOUS PSYCHOLOGICAL DISORDERS.

WHAT THIS APP DOES, IF A PERSON IS SHOPPING FOR A PARTICULAR DRUG, IT TAKES A PICTURE OF THE PILL, THE LITERAL PICTURE OF THE PILL I'M SHOWING HERE, IT STORES IT IN EXTERNAL DEVICE SO NEXT TIME IT'S FASTER TO SHOW THIS PICTURE.

NOW IMAGINE THERE IS AN AD RUNNING IN A DIFFERENT APP ON THE SAME DEVICE.

OKAY?

IT HAS BAD SHOWING THAT WOULD BE A TOTALLY RANDOM ACT.

IT HAS THOG TO DO WITH THE PHARMACY SHOPPING APP THAT I SHOWED YOU BEFORE.

HOWEVER AS I TOLD YOU BEFORE, AN AD BEING SHOWN ON IT HAS THE ABILITY TO ASK A VERY SIMPLE QUESTION.

DOES A FILE WITH A PARTICULAR

NAME EXIST ON THE EXTERNAL

STORAGE?

AND IN THIS CASE, IT'S ASKING

FOR A FILE WHOSE NAME

CORRESPONDS TO THE IMAGE OF ONE

OF THE ANXIETY DRUGS.

SO WHAT CAN A MOBILE AD, AND

THIS IS A QUESTION TO YOU GUYS,

WHAT CAN A MOBILE AD LEARN FROM

THE ANSWER TO THIS QUESTION?

SO ALL IT LEARNS IS ONE BIT.

IF THE FILE WITH A PARTICULAR

NAME EXISTS ON THE DEVICE.

WHAT CAN THE AD LEARN BY KNOWING

THE ANSWER?

>> IF YOU ORDERED OR YOU USE --

>> THE ONLY REASON A -- IF THE

ANSWER TO THAT QUESTION IS YES,

THE ONLY REASON A FILE WITH THIS

NAME WOULD HAVE EXISTED ON THIS

DEVICE IS THE USER USED THAT APP

AND SEARCHED FOR THAT DRUG.

THERE IS NO OTHER REASON.

SO THAT IF THEY SEE AN AD -- IF
AN AD SEES THAT THE FILE LIKE
THIS EXISTS I IT CANNOT READ
THIS FILE.
IT LEARNS WITH 100% CERTAINTY
BECAUSE THIS NAME IS UNIQUE THAT
THE PERSON HAS BEEN SHOPPING FOR
A PARTICULAR DRUG.
AND THIS TURNS OUT TO BE A
PERVASIVE PROBLEM.
BECAUSE -- AND REMEMBER, THIS AD
IS BEING SHOWN IN A TOTALLY
DIFFERENT APP.
IT IS SHOWN IN AN AD WHICH IS
RUNNING ON THE DEVICE, MAYBE
EVEN LATER NOT THE TIME OF THE
PHARMACY SHOPPING APP.
IF THERE IS AN APP THAT NEED NOT
EVEN BE ADVERTISING SUPPORTED
THAT PUTS FILES INTO EXTERNAL
STORAGE LIKE A LOT OF THEM DO
THAT DEPEND ON THE USER BEHAVIOR
THAT AN AD CAN DETERMINE THIS

FILE EXISTS AND THE FACT THAT

THIS FILE EXISTS IT CAN INFER

WHAT USER BEHAVIOR LED TO THE

PRESENCE OF THESE FILES.

SO I SHOWED THE EXAMPLE WITH

DRUGS.

AND BY THE WAY, THIS VIOLATES

NOTHING IN THE SECURITY POLICY

BECAUSE ALL THE SECURITY POLICY

SAYS IS THAT IT CANNOT READ

THESE FILES.

AND IT CANNOT.

IT DOES NOT READ THE FILE.

IT JUST LEARNS THAT THE FILE

EXISTS.

AND THIS ACTUALLY TURNS OUT THAT

THIS AFFECTS ALL KINDS OF MOBILE

APPS.

HERE IS ANOTHER APP, THIS

HAPPENS TO BE A MOBILE WEB

BROWSER WHICH CACHES IN FILES

WITH PREDICTABLE NAMES, DERIVED

FROM THE URL THAT THE USER

VISITED.

A MALICIOUS AD RUNNING IN A

DIFFERENT APP CAN FIGURE OUT

WHICH SITES THE USER VISITED

RECENTLY.

BECAUSE THE ONLY REASON A FILE

OF THAT NAME WOULD APPEAR ON THE

DEVICE IS IF IT WERE CACHED BY

THE USER'S MOBILE BROWSER AS A

RESULT OF A VISIT TO A

PARTICULAR WEBSITE.

OUR ARTICLE HAS AN EXAMPLE OF

MANY OTHER INSTANCES, AN

ANALYSIS OF SEVERAL ADVERTISING

LIBRARIES, WHICH HAS A VERY

SIGNIFICANT PORTION OF ANDROID

APPS, THEY ALL AT LEAST AT THE

TIME OF OUR STUDY, I'LL TELL YOU

IN A SECOND WHAT HAPPENED LATER,

HAD THIS VULNERABILITY, MEANING

A MOBILE AD COULD INFER

INFORMATION ABOUT THE USER

BECAUSE OF PRESENCE OF FILES

USED BY THE USER.

THE LEAKAGE OF LOCATION

INFORMATION, I'M NOT GOING TO GO

MUCH INTO DETAIL ABOUT THIS,

I'LL JUST SHOW YOU THIS PICTURE

AND THE ONLY THING I WAND TO

ADMIRE ABOUT THIS PICTURE IS HOW

COMPLEX IT IS.

BECAUSE IT SHOWS LIKE HOW IN

FIVE STAGES, LITERALLY, IN

MOPUB, INFORMATION ABOUT THE

USER'S LOCATION CAN BE FOUND,

AND A MOBILE APP RUNNING IN

MOPUB, IMMEDIATELY REVEALS A TOL

TON OF INFORMATION ABOUT THE

USER, LIKE INFORMATION ABOUT A

SINGLE FAMILY RESIDENCE WHERE

THE USER LIVES.

THIS INFORMATION CAN LEAK OUT

THROUGH THIS INTERACT CHANNELS.

OKAY, WHAT ARE THE LESSONS OF

THIS STUDY?

AS FAR AS I KNOW, THIS IS THE

FIRST REASONABLY COMPREHENSIVE
STUDY OF FIRST, HOW ADVERTISING
LIBRARIES ON ANDROID TRY TO
PROTECT USERS FROM MALICIOUS
MOBILE ADS AND SNOOPING MOBILE
ADS WITH INTERMITTENT SUCCESS AS
YOU CAN SEE.
IT SHOWS AND THIS IS A SLIGHTLY
MORE TECHNICAL RESULTBUT
NEVERTHELESS AS IMPORTANT, THAT
STANDARD WEB ISOLATION POLICIES
THAT ARE USED IN WEB BROWSERS
HERE EXACTLY THE SAME THINGS
USED IN THE MOBILE CONTEXT, THEY
NO LONGER PREVENT LEAKAGE OF
SENSITIVE INFORMATION, SOMETHING
MORE SUBTLE IS NEEDED HERE.
WE ACTUALLY WHEN WE FIRST DID
THIS STUDY LAST SUMMER WE DIDN'T
MAKE IT PUBLIC RIGHT AWAY
BECAUSE WE WANTED TO WORK WITH
DEVELOPERS OF THIS ADVERTISING
LIBRARIES AND COMPANIES THAT

DEPLOY THEM.

SO THAT THEY CAN FIX AT LEAST

THE MOST SEVERE VULNERABILITIES

THAT WERE IDENTIFIED AND IN

FACT, SOME OF THEM DID, IN

PARTICULAR ADMOB, ACTUALLY OWNED

BY GOOGLE, THEY FIXED IT IN THE

LATEST RELEASE OF THEIR ADDDIS

DECAY.

SOME ADVERTISERS TOLD US TO GO

AWAY AND NOT BOTHER THEM

ANYMORE.

I HOPE THEY WILL DO THIS AFTER

THIS TALK.

THIS PAPER IS WRITTEN FOR A

TECHNICAL COMPUTER SCIENCE

AUDIENCE BUT I HOPE THE BIG

THEMES WILL COME ACROSS FROM

THAT.

THANKS.

[APPLAUSE]

>> SO NEXT WE'LL HAVE FLORIAN

SCHAUB, HE IS A POSTDOC FELLOW

CURRENTLY AT CARNEGIE MELLON.

>> THAT IS CORRECT.

HELLO EVERYONE.

I'M GOING TO BE TALKING ABOUT A PROJECT CALLED THE USABLE PRICE OF POLICY PROJECT, LARGE SCALE PROJECTS FUNDED BY THE NSF, AND I'M A POSTDOC IN THIS PROJECT NORMAN IS ACTUALLY THE LEAD PI IN THIS PROJECT AND A COLLABORATION BY MANY PEOPLE AT CMU, FORDHAM, THE SOCIETY FOR INTERNAL STANDARDS AT STANFORD.

I'M GOING TO GIVE YOU A SHORT MOTIVATION AND GIVE YOU AN OVERVIEW OF WHAT WE DO IN THIS PROJECT IN DIFFERENT PARTS.

WE LOOK AT PRIVACY POLICIES AND PRIVACY POLICIES ORIGINALLY HAD THIS PROMISE OF SERVICE PROVIDERS WOULD DISCLOSE THE DATA SERVICES, USERS COULD MAKE INFORMED CHOICES ABOUT WHICH

PROVIDERS OR WEBSITES THEY TRUST

WITH THE DATA BUT THE REALITY

LOOKS A LITTLE BIT DIFFERENT.

BECAUSE PRIVACY POLICIES PLAY

DIFFERENT ROALTS.

IT'S NOT ABOUT -- ROLES.

FOR USERS WHEN THEY DRAFT A

PRIVACY POLICY THE GOAL IS TO

DEMONSTRATE LEGAL AND REGULATORY

COMPLIANCE AND THERE WAY, LIMIT

THEIR LIABILITY.

AND REGULATORS ARE HAPPY ABOUT

THIS.

THEY USE THESE PRIVACY POLICY TO

ASSESS AN ENFORCE COMPLIANCE.

A STRONG INTERACTION BETWEEN

THOSE TWO PLAYERS MEANS THE USER

KIND OF DUETS LEFT OUT.

AS A RESULT THESE PRIVACY

POLICIES ARE LONG COMPLEX

DIFFICULT TO UNDERSTAND FULL OF

JARGON THEY DON'T REALLY OFFER

MANY CHOICES TO USERS.

AND I THINK WE ALL KNOW BY NOW
THAT USERS MAINLY IGNORE THEM.
AND THIS PUTS US IN THIS REALLY
WEIRD SITUATION WHERE THESE
POLICIES OUTLINE WHAT COMPANIES
DO WITH OUR DATA AND WHAT WE
ALLOW THEM TO DO WITH OUR DATA.
BUT THIS INFORMATION IS NOT USED
BY THE USERS OR MADE -- OR IT'S
YEAH APPARENT TO THEM.
AND THERE HAS BEEN MUCH WORK ON
OVERCOMING THE STATUS QUO HERE.
PROPOSALS LIKE PRIVACY POLICIES
SHOWING SHORT SUMMARIES OF
POLICIES GRAPHICAL APPROACHES AS
WELL AS MACHINE READABLE PRIVACY
POLICIES.
BUT MANY OF THESE APPROACHES
DON'T GO ANYWHERE REALLY BECAUSE
THEY LACK INDUSTRY SUPPORT AND
THERE'S NOT SUFFICIENT ADOPTION
INCENTIVES FOR COMPANIES TO
ACTUALLY IMPLEMENT THOSE

SOLUTIONS THAT HAVE BEEN

PROPOSED.

THIS IS REALLY WHERE OUR PROJECT

COMES IN.

BECAUSE WE ARE LOOKING AT SEMI

AUTOMATICALLY ANALYZING THE

ESSENTIAL LANGUAGE PRIVACY

POLICIES THAT MOST WEBSITES,

MOST MOBILE APPS ALREADY HAVE

AND WE ANALYZE THEM TO THEN

EXTRACT KEY DATA PRACTICES OUT

OF THESE POLICIES, AND WE DO

THIS BY EXTRACTING CROWD

RESOURCES AND IN THIS WAY ENABLE

LARGE SCALE IMIZ, MODELING USERS

PRIVACY PREFERENCES AND CONCERNS

SO WE CAN PROVIDE THEM MORE

EFFECTIVE NOTICES THAT FOCUS ON

THOSE INFORMATION ASPECTS AND

DATA PRACTICES USERS REALLY CARE

ABOUT AND GIVE THEM INFORMATION

THAT IS ACTIONABLE.

OUR PROJECT HAS MANY TIGHTLY

INTERCONNECTED THREADS AND I'M
NOT GOING TO TRY TO UNTANGLE
THIS FOR YOU RIGHT NOW, YOU CAN
LOOK AT THE REPORT TO GET A
DEEPER UNDERSTANDING.
OUR GOAL IS TO BETTER INFORM
USERS, WE WANT TO GIVE THEM
NOTICES THAT ACTUALLY INFORM
THEM AND PROVIDE THEM WITH
CHOICES AND WE WANT TO INFORM
PUBLIC POLICY BY SHARING ISSUES
WITH PRIVACY POLICIES AS WELL AS
SHOWING WAYS OF REMEDYING THOSE
ISSUES AND ALSO PROVIDING HOPE
BETTER FLOWS COULD BE PROVIDED.
AND TO IDENTIFY DATA PRACTICES
OF INTEREST, WE APPROACH THIS
REALLY FROM DIFFERENT
PERSPECTIVES.
PART OF OUR RESEARCH TEAM LOOKS
AT LEGAL ANALYSIS.
JOEL R EVERYBODYIDENBERG AND HIS
TEAM, SEE WHAT ISSUES COME UP

THE MOST.

WE CONDUCT USER STUDIES WHERE WE DETERMINE WHAT OUR PRIVACY PRACTICES CONCERNS AND EXPECTATIONS OF USERS AND ASHWINI THIS MORNING TALKED ABOUT SOME EXPECTATION IN THAT CONTEXT.

AND WE ALSO LOOK AT THE POLICIES THEMSELVES.

HOW ARE THEY WRITTEN?

HOW DATA PRACTICES ACTUALLY EXPRESS IN THOSE POLICIES AND WE HAVE SOME WORK GOING ON RIGHT NOW THAT LOOKS AT QUANTIFYING THE AMBIGUITY AND PRIVACY POLICIES.

TO ANALYZE THESE POLICIES, WE STARTED BY BUILDING AN ANNOTATION TOOL THAT BASICALLY ALLOWS US TO GIVE POLICIES TO CROWD WORKERS OR OTHER ANNOTATORS, AND THIS TOOL SHOWS

THEM THE POLICY TON LEFT HAND

AND A QUESTION ON THE RIGHT.

WE ASK THEM TO ANSWER THE

QUESTION BUT ALSO MARK TEXT THAT

BASICALLY PROVIDES THE EVIDENCE

FOR THE ANSWER.

AND THIS IS REALLY IMPORTANT

BECAUSE THIS TEXT SELECTION IN

COMBINATION WITH THE ANSWER THEN

HELPS US.

MACHINE MOLDS.

SHOWING THESE TASKS TO MULTIPLE

ANNOTATORS WE CAN ACTUALLY GET

QUITE ROBUST RESULTS.

HOWEVER JUST GIVING THIS TO SOME

SWERG CROWD WORKERS AND SAY WELL

TEN PEOPLE SAY THAT'S OKAY IS

NOT REALLY A GOOD IDEA.

SO WE CONDUCTED STUDIES TO

COMPARE THE PERFORMANCE

ANNOTATION PERFORMANCE OF

EXPERTS WHO EITHER WRITE

POLICIES OR HAVE LONG EXPERIENCE

IN ANALYZING POLICIES.

GRADUATE STUDENTS IN LAW AND PUBLIC POLICY AND ENTERING CROWD WORKERS, RECRUITED FROM AMAZON, AND THE CROWD WORKERS AND -- ARE SKILLED ANNOTATORS, ANNOTATE26 POLICIES.

I'M NOT GOING TO GO TOO MUCH INTO THE DETAILS FOR THE SAKE OF TIME BUT ONE OF THE INTERESTING RESULTS IS EVEN THE EXPERTS DON'T ALWAYS AGREE ON THE INTERPRETATION OF A PRIVACY POLICY.

AND ONE REASON FOR THAT IS THAT THE POLICIES ARE VAGUE BUT SOMETIMES CONTRADICTORY.

TOO MANY CONTEXTS HANDLED IN THE POLICY.

GOOD NEWS FOR DATA COLLECTION PROCESSES THOSE ARE RELATIVELY EASY TO IDENTIFY AND EXTRACT BUT DATA SHARING PROCESSES ARE MORE

COMPLEX.

THEY ARE SPREAD OUT THROUGHOUT

THE POLICY, SHARING IS

IDENTIFIED IN MANY DIFFERENT

PARTS OF THE POLICIES.

IT IS DIFFICULT TO EXTRACT FINER

NUANCES.

SKILLED ANNOTATORS WE FIND QUITE

ENCOURAGING RESULTS.

WHEN WE HOLD THE CROWD WORKERS

TO A CERTAIN STANDARD, 80%

AGREEMENT, WHICH MEANS EIGHT OUT

OF TEN HAVE TO COME UP WITH THE

SAME INTERPRETATION, THESE CROWD

WORKERS AGREE WITH THE

INTERNTION THAT OUR CRED

STUDENTS DO AS WELL.

THEY COME UP WITH AN ACCURATE

INTERPRETATION, IN ALMOST ALL OF

THE OTHER CASES THEY DON'T REACH

AGREEMENT WHICH MEANS THEY DON'T

GIVE US WRONG ANSWERS.

WE HAVE THE STARK BAR SHOWS US

AS A PERCENTAGE WHERE THEY COME TO A DIFFERENT CONCLUSION THAN THE SKILLED ANNOTATORS.

WHICH IS GREAT.

WE EITHER GET AN ANSWER FROM OUR CROWD WORKERS WITH A HIGH LIKELIHOOD IT IS ACTUALLY CORRECT OR WE MAY NOT GET AN ANSWER, WHICH TELLS US THE POLICY MAY BE VAGUE ON THE PARTICULAR ISSUE WE ARE TRYING TO ANALYZE.

SO THIS SHOWS THAT ACCURATE CROWD SOURCING OF PRIVACY POLICIES IS FEASIBLE BUT PRIVACY POLICIES ARE STILL LONG AND COMPLEX.

SO WE LOOK AT LEVERAGING MACHINE LEARNING NATURAL LANGUAGE PROCESSING TO FURTHER ENHANCE THOSE EXTRACTION TASKS AND MAKE IT EASIER FOR CROWD WORKERS TO COMPLETE THESE TASKS FASTER

WITHOUT LOSS OF ACCURACY.
AND ONE THING WE HAVE BEEN
DEVELOPING HERE, WE TAKE THE
ANSWER WE TAKE FROM OUR SKILLED
ANNOTATORS, AND USE THEM FOR
REIVELS MODELS FOR DIFFERENT
DATA PREFERENCES WE WANT TO
EXTRACT AND WE HIGHLIGHT THE TOP
FIVE TOP TEN PARAGRAPHS THAT
MOST LIKELY CONTAIN ANSWERS OR
INFORMATION ABOUT THE DATA
PRACTICES WE WANT TO EXTRACT.
WHAT WE FIND THAT REALLY HELPS
THE ANNOTATOR TO COME TO
SECLUSIONS FASTER WITHOUT
LOSING -- WITHOUT AFFECTING THE
ACCURACY.
AND THIS, WE DID ADDITIONAL
EXPERIMENTS WHERE OR ANALYSIS
WHERE WE LOOKED AT DO THEY
ACTUALLY JUST FOCUS ON THOSE
FIVE PARAGRAPHS OR DO THEY ALSO
READ OTHER PARTS?

AND THEY DO READ OTHER PARTS OF
THE POLICY BUT IT HELPS THEM TO
FOCUS THEIR SEARCH AND FIND
PARTS OF THE POLICY AGAIN.
ANOTHER THING WE DO IS WE SPLIT
UP THIS RELATIVE COMPLEX TASK OF
READING A PRIVACY POLICY, GIVING
A CROWD WORKER ONLY A SINGLE
PARAGRAPH.
WE CAN FURTHER SPLIT THOSE TASKS
AS WELL SO RATHER THAN ASKING
THEM MULTIPLE QUESTIONS AS ONCE,
WE FIRST ASK ONE SET OF CROWD
WORKERS TO KIND OF LABEL IN WHAT
CATEGORY OF DATA PRACTICE IS
DESCRIBED, SHARING PRACTICE,
COLLECTION PRACTICE, MAYBE ABOUT
USER ACCESS AND THEN IN
FOLLOW-UP QUESTIONS WE CAN ASK
MORE DETAILS THAT ARE -- THAT IS
THE PARTICULAR ASPECTS FOR THAT
KIND OF CATEGORY.
AND THAT MEANS THAT THE TASK

INTERFACES WE CAN SHOW TO CROWD
WORKERS A LOT MORE COMPACT AND
THEY CAN COMPLETE THOSE TASKS
FASTER AND WITH LOWER ERRORS.
AND BASED ON THAT WE HAVE
DEVELOP AND ANNOTATION SCHEME
THAT REALLY MAKES USE OF THIS
APPROACH.
THIS IS AN INTERFACE NOT FOR
CROWD WORKERS, USING THIS WITH
LAW STUDENTS BUT THE NEXT STEP
IS TO BREAK THIS UP AGAIN WITH
THE APPROACH I JUST OUTLINED BUT
THIS IS A VERY FINE GRAINED
ANNOTATION APPROACH AND
CURRENTLY COLLECTING DATA FROM
LAW STUDENTS WHERE WE ALREADY
HAVE OVER 100 POLICIES ANNOTATED
AND SUPPLIES A REALLY RICH
PICTURE ON HOW INFORMATION IS
REPRESENTED HOW DATA PRACTICES
ARE REPRESENTED IN THE POLICIES.
WE'RE GOING TO RELEASE A DATA

PORTAL TO ALLOW EXPORTATION OF
THIS DATA ON JANUARY 28th, SO
VISIT OUR WEBSITE TOWARDS THE
END OF THE MONTH.
AND THE NICE THING ABOUT THIS
DATA IS IT'S REALLY HELPFUL TO
TRAIN MACHINE LEARNING AND
NATURAL LANGUAGE PROCESSING
MODELS AND TRY FREE SESSION IN
THIS AREA.
ULTIMATELY WHAT WE WOULD BE
HOPING FOR IS THAT WE CAN
ACTUALLY AUTOMATE THE EX
EXTRACTION.
PARAGRAPH SEQUENCE ALIGNMENT, IF
I HAVE A PARAGRAPH IN AMAZON
POLICY I KNOW THIS ONE IS ABOUT
COLLECTION OF CONTACT
INFORMATION AND THAT IF I
COMPARE THAT ONE TO, THAT
PARAGRAPH TO OTHER PARAGRAPHS
AND OTHER POLICIES, THERE IS A
HIGH LIKELIHOOD THAT I CAN FIND

SIMILAR PARAGRAPHS THAT ALSO
DESCRIBE THE COLLECTION OF
CONTACT INFORMATION, AND THIS
WAY, WE CAN BASICALLY REDUCE
WHICH PARAGRAPHS MIGHT EVEN HAVE
TO SHOW TO CROWD WORKERS AND
THIS WAY AUTOMATE SOME OF THE
ANNOTATIONS AND ANALYSIS.

NOW, WHEN ONCE WE HAVE ALL THIS
DATA WE WANT TO PROVIDE NOTICE
TO USERS AND HERE REALLY FOCUS
ON MAKING SURE THE INFORMATION
WE GIVE YOU IS ACTUALLY
RELEVANT, SO WE HIGHLIGHT
UNEXPECTED PRACTICES, PRACTICES
USERS CARE ABOUT AND INFORMATION
SHOULD BE ACTIONABLE.

IF USERS CAN'T MAKE A CHOICE
THEN THERE'S NO POINT IN SHOWING
THEM INFORMATION.

BECAUSE YOU ARE JUST GOING TO BE
HELPLESS.

YOU HEARD ABOUT THIS THIS

MORNING, ABOUT USERS BEING

RESIGNED BECAUSE THEY CAN'T

ACCESS ANY CHOICES.

SHOW THE LABEL CHOICES THAT ARE

MADE AVAILABLE, THERE AREN'T

THAT MANY BUT BECAUSE WE CAN

SCALE UP THIS ANALYSIS TO MANY

WEBSITES WE CAN SHOW MORE

POLICIES TO WEBSITES AS

ALTERNATIVES TO USERS.

AND THIS WAY OFFER THEM CHOICES

THAT GO BEYOND WHAT THE POLICY

OF A SINGLE WEBSITE MIGHT OFFER.

AND WE'RE CURRENTLY A PROCESS OF

A BROWSER PLUG IN TO BASICALLY

MAKE THIS TECHNOLOGY AVAILABLE

TO USERS.

AND IT IS A LIMITED SET OF

RELEVANT PRACTICES AND WE ARE

GOING THROUGH AN IT RATIVE -- ITERATIVE

PROCESS, THAT WE HOPE TO BE ABLE

TO SHOW TO THE PUBLIC THIS

SUMMER.

IN SUMMARY, WE DO THIS WITH

CROWD SOURCING, NATURAL LANGUAGE

PROCESSING AN MACHINE LEARNING.

THE GOAL OF OUR PROJECT IS

REALLY TO ENABLE LARGE SCALE

ANALYSIS OF THESE PRIVACY

POLICIES, AT THE SAME TIME, WE

ARE ANNOTATING 100, BY THE END

OF THE YEAR WE HOPE TO BE

ANNOTATING A THOUSAND POLICIES,

FOCUS AND ASSIST BUT ALSO HELP

REGULATORS THEIR FACILITIES,

USERS CARE ABOUT OR ARE

CONCERNED WITH.

AT THE SAME TIME WE WANT TO SHOW

WAYS TO EFFECTIVELY INFORM USERS

ABOUT THE DATA PRACTICES THAT

ARE CURRENTLY LOSS IN THOSE

POLICIES.

NO ONE'S GOING TO READ THE

POLICIES SO IF WE WANT TO MAKE

THOSE POLICIES USABLE WE NEED TO

EXTRACT THE INFORMATION THAT IS

REALLY RELEVANT TO USERS AND
SHOW THEM IN A FORM THAT
ACTUALLY MAKES SENSE TO THEM AND
ACTUALLY ALLOWS THEM TO ACT ON
IT.

[APPLAUSE]

>> AND OUR LAST PRESENTER OF THE
DAY WILL BE NORMAN SADEH, NORMAN
IS A PROFESSOR IN THE COMPUTER
SCIENCE DEPARTMENT AND CARNEGIE
MELLON.

>> GOOD AFTERNOON.

I THINK VERY FEW PEOPLE IN THIS
AUDIENCE PROBABLY APPRECIATE HOW
MUCH PROGRESS WE HAVE BEEN ABLE
TO MAKE OVER THE PAST FEW YEARS
IN BOTH MODELING AND PREDICTING
PEOPLE'S PRIVACY PREFERENCES.

DEVELOPING PERSONALIZED PRIVACY
ASSISTANCE, THE SUCCESS WE HAVE IT.

THIS IS JOINT WORK WITH A LARGE
TEAM THAT WILL BE ACKNOWLEDGED
ON THE VERY LAST SLIGHT.

I DON'T THINK I'M 0 GOING TO
HAVE TO WORK VERY HARD TO
CONVINCE THIS AUDIENCE THAT
PEOPLE CARE ABOUT PRIVACY.
AND YET, AS WE KNOW ALSO PEOPLE
ARE VERY PRIZED WHEN YOU TELL
THEM WHAT SORTS OF APPS THEY
HAVE DOWNLOADED ON THE MOBILE
PHONES AND WHAT INFORMATION IS
SHARED BY THESE APPS.
THIS IS JUST AN EXAMPLE OF AN
EARLY STUDY THAT WE CONDUCTED IN
THE SURFACE.
THE BIGGEST OFFENDER WAS AN APP
THAT SOME IN THE FTC ARE
FAMILIAR WITH, AND BRIGHTEST
FLASHLIGHT WAS ONE THAT WE'RE
FAMILIAR WITH.
AND AS WE ALL KNOW AND WE JUST
EMPHASIZE, VERY FEW PEOPLE READ
PRIVACY POLICIES AND THAT'S PART
OF THE REASON WHY WE HAVE THIS
LEVEL OF SURPRISE.

ALSO AS I COULDN'T THINK WE ALSO

REALIZING, MANY OF US HAVE TONS

AND TONS OF SETTINGS AND JUST

DON'T HAVE THE TIME TO CONFIGURE

ALL OF THESE SETTINGS.

FOR INSTANCE IF YOU ARE A

SMARTPHONE USE AND AS MOST

SMARTPHONE USERS YOU HAVE

BETWEEN 50 AND 100 APPS ON YOUR

PHONE AND THESE REQUIRE THREE

AND FOUR PERMISSIONS SO ACCESS

YOUR MORE SENSITIVE INFORMATION.

IF YOU DO THE MATH YOU REALIZE

THIS WOULD REQUIRE PEOPLE TO

CONFIGURE AROUND 1350 DIFFERENT

SETTINGS.

HOW MANY PEOPLE ARE WILLING TO

CONFIGURE 150 SETTINGS ON THEIR

CELL PHONE?

NOT THAT MANY.

SO WITH THIS IN MIND, AND

OBVIOUSLY WITH RECOGNITION OF

THESE CHALLENGES BOTH ALREADY ON

THE FIXED INTERNET AND IN THE
MOBILE SPACE, THE NATURAL
QUESTION IS WELL, IF THIS
ALREADY DOESN'T WORK ON THE
FIXED WEB, IF THIS ALREADY
DOESN'T WORK ON THE MOBILE WEBB
WHAT ARE THE CHANCES THAT IT'S
GOING TO WORK IN IOT, WITH "THE
INTERNET OF THINGS."
SO OUR SPACE LEAVES THIS IDEA
THAT PERHAPS PERSONALIZED
PRIVACY ASSISTANTS COULD BE
DEVELOPED TO REDUCE THE EXPWURD
IMPLORE YOU TO MANAGE YOUR
PRIVACY BETTER ACROSS THESE
DIFFERENT ENVIRONMENTS.
SO THE IDEA IS THAT THESE
PERSONALIZED PRIVACY ASSISTANTS,
IN PARTICULAR WE LEARN OVER TIME
YOUR PRIVACY PREFERENCES AND WE
WILL BE ABLE TO CONFIGURE MANY
OF THOSE SETTINGS BASED ON
VARIOUS CORRELATIONS BETWEEN HOW

YOU FEEL ABOUT SHARING YOUR INFORMATION WITH ONE APP VERSUS ANOTHER AND ALSO UNDERSTANDING WHAT YOUR EXPECTATIONS ARE GOING BACK TO THE PRESENTATION THAT WAS GIVEN THIS MORNING BY A SHWINI, WHO HAS BEEN LOOKING AT THESE ISSUES, AND AS FLEURION MENTIONED, WHEN YOU READ THE PRIVACY POLICIES THEY ARE LONG AND VERBOSE BUT THERE'S ONLY A SMALL AMOUNT THAT MATTERS TO YOU AND A TINIER FRACTION OF THE TEXT THAT PERTAINS TO THINGS THAT YOU DIDN'T ALREADY EXPECT SO PERHAPS THE PERSONALIZED PRIVACY ASSISTANTS COULD HELP US BY HIGHLIGHTING THOSE ELEMENTS OF POLICIES THAT WOULD REALLY BE A SURPRISE TO US AND LEAD TO US MODIFY OUR BEHAVIOR AS WE ENTER A SMART ROOM FOR INSTANCE IN AN IOT CONTEXT.

PERHAPS THESE ASSISTANTS COULD
ALSO HELP MOTIVATE USERS TO
REVISIT THEIR SETTINGS AND
VERIFY THEY STILL FEEL THE SAME
WAY.
PRIVACY SETTLE REHABILITATION
NOT FIXED BASED ON EXPERIENCE
AND WHAT YOU LEARN.
SO AGAIN WHAT I WOULD LIKE TO DO
IS SHARE SUCCESS SUPPORTING THE
EARLY ELEMENTS OF THIS
FUNCTIONALITY.
WHAT YEAR'S SEEING HERE IS AN
EARLY MODEL THAT WE BUILD ABOUT
HOW PEOPLE FELT SHARING THEIR
INFORMATION WITH VARIOUS MOBILE
APPS FOR VARIOUS STEPS OF
PURPOSES WHETHER THE APP
REQUIRED THIS INFORMATION FOR
INTERNAL PURPOSES, FOR SHARING
WITH ADVERTISING NETWORKS, FOR
PROFILING PURPOSES OR SHARING
WITH SOCIAL NETWORKS.

I'M NOT GOING TO DESCRIBE THIS
CHART IN GREAT DETAIL BUT WHAT
WE'RE SUPPOSED TO SEE SHEER IS
THAT PEOPLE DON'T ALWAYS FEEL
THE SAME WAY ON ANNAL WHEN IT
COMES TO SHARING THEIR
INFORMATION.
THERE ARE CLEARLY DIFFERENCES
BETWEEN SHARING YOUR LOCATION
INFORMATION AT A FINE LEVEL
VERSUS A COARSE LEVEL AND
DIFFERENCES IN SHARING ACCESS TO
SMS FUNCTIONALITY AND WHAT
WHETHER YOU ARE DOING THAT FOR
ADVERTISING PURPOSES VERSUS
USING IT PURELY FOR THE PURPOSE
OF THE APP THAT YOU'RE TRYING TO
DOWNLOAD.
PEOPLE WILL THINK DIFFERENTLY.
WHAT THE FIGURE DOESN'T SHOW IS
THE DIFFICULTY IN CONFIGURING
THE SETTINGS.
THE REASON IS THAT THIS CHART IS

NOT THE WHOLE STORY.
THE WHOLE STORY COMES OUT WHEN
YOU LOOK AT THE OTHER CHART
WHICH SHOWS YOU THE STANDARD
DEVIATION WHEN IT COMES TO THESE
PREACHERSEST PREACHERSES AND THE
STORY HERE AND THE REASON THAT
PRIVACY IS TO COMPLEX IS THAT WE
DON'T ALL FEEL THE SAME WAY
ABOUT THESE ISSUES F WE DID IT
WOULD BE EASY TO COME UP WITH
DEFAULTS AND IT WOULD BE DONE
AND THE FIREFIGHT COULD SAY WE
DON'T FEEL COMFORTABLE ABOUT
THIS.
BUT CLEARLY THAT'S NOT THE WAY
WE OPERATE.
THE REASON THIS IS COMPLICATED
IS BECAUSE THE DIVERSITY IN
PREFERENCES.
SOME ARE FINE WITH THEIR
INFORMATION SHARED WITH
ADVERTISERS AND THE OTHERS

OBJECT.

THE GOOD NEWS AND THIS IS A

RESULT THAT HAS RESULTED IN

RESEARCH IN THE PAST FEW YEARS

IS THAT VERY OFTEN IT IS

POSSIBLE TO ORGANIZE THE

POPULATION AND THEIR PREFERENCES

IN TO A FAIRLY SMALL GROUPS OF

PEOPLE, GROUPS OF PEOPLE THAT

FEEL VERY MUCH THE SAME WAY

ABOUT THESE ISSUES.

SO WHAT I WANT TO SHARE WITH YOU

HERE IS AGAIN AN EARLY EXAMPLE

OF OUR WORK, WHERE AGAIN WE'RE

LOOKING AT THE MOBILE APP

PERMISSION PREMPSES AND WE'RE

ABLE TO ORGANIZE A USENERS FOUR

GROUPS AND BASED UPON THESE FOUR

GROUPS AND WHAT WE'RE ABLE TO

PREDICT BASED ON THE PRERCHTSES

IN THE FOUR GROUPS WE'RE ABLE TO

SHOW THAT IT MIGHT BE POSSIBLE

TO PREDICT BETWEEN 75 AND 85% OF

THEIR PRIVACY PRACTICES WHEN IT
CAME TO CONFIGURING THEIR
PERMISSION SETTINGS.
THIS IS VERY, VERY SIMPLE
TECHNOLOGY.
I'M GOING TO SHOW YOU THAT WE WE
HAVE BEEN ABLE TO GO FURTHER
THAT HAPPEN THAT.
THAT GIVES YOU SENSE FOR HOW
EASY IT IS TO PREDICT MANY
DIFFERENT SETTINGS THAT PERHAPS
PEOPLE WOULD WANT TO HAVE.
SO THIS NEXT CHART HERE SHOWS
YOU THE NEXT STEP IN OUR
RESEARCH WHERE WE LOOKED AT
ACTUALLY A POPULATION OF 240,000
USERS, A I SHOULD SAY 3 MILLION
USERS BUT WE HAD TO CLEAN UP THE
DATA QUITE A BIT AND EVENTUALLY
ZOOMED IN NOT THAT I KNOW THE
FRACTION.
THE POPULATION MOST ENGAGED WITH
THE PERMISSION SETTLINGS AND

THESE ARE THE LBE USERS.
IT WAS AN EARLY VERSION OF
ANDROID WHERE USERS COULD
CONFIGURE MANY DIFFERENT
SETTLINGS AND WE'RE ABLE TO SHOW
THROUGH PROFILE AND PERSONALIZED
LEARNING WE COULD JUST BY ASKING
PEOPLE A SMALL NUMBER OF
QUESTIONS EFFECTIVELY PREDICT
MOST OF THE SETTINGS THAT THEY
WOULD NEED TO CONFIGURE ON THEIR
SMARTPHONES FOR THE APPS THEY
WERE GOING TO DOWNLOAD.
IF YOU WERE TO SIX THEM SIX
QUESTIONS YOU COULD EFFECTIVELY
REACH A LEVEL OF ACCURACY OF
ABOUT 92%, IF YOU'RE WILLING TO
DOUBLE THE NUMBER OF QUESTIONS
ASKED YOU'RE GETTING CLOSE TO
95%.
NOW WE ARE NOT SUGGESTING IN ANY
WAY THAT YOU SHOULD FULLY
AUTOMATE THE SETTING OF PRIVACY

PERMISSIONS.

WE STRONGLY BELIEVE THAT IT'S TO
THE USERS AND THERE ARE CLEAR
SITUATIONS WHERE THE USERS
FEESTLES A CERTAIN WAY ABOUT A
SETTING AND YOUR MODEL IS NOT
ALWAYS GOOD ENOUGH TO PREDICT SO
THAT'S WHERE YOU SHOULD ASK THE
USER AND WHAT WE'RE ADVOCATING
SO WE HAVE GONE ONE STEP FURTHER
AND WE WORKED WITH REAL USERS ON
THEIR ACTUALLY CELL PHONES AND
WE DEVELOP PROFESSIONALS.

WE CAME UP WITH SEVEN DIFFERENT
PROFILES AND ASKED PEOPLE TO
DOWNLOAD THIS EARLY VERSION OF A
PERSONALIZED PRIVACY ASSISTANCE
AND IT WOULD AND THEM THREE TO
FIVE QUESTIONS BASED ON THE APPS
AND BASED ON THE ANSWERS IT
WOULD RECOMMEND SETTLINGS AS YOU
CAN SEE ON THE RIGHT-HAND SIDE
OF THE SLIDE IN FRONT OF YOU.

SO WE RAN THIS AND TO MAKE A

LONG STORY SHORT WE RAN THESE

FOR A PERIOD OF 10 DAYS. THE

LAST SIX DAYS OF THE STUDY WE

TRIED TO SEE IF WE COULD NUDGE

USERS

USERS TO MODIFY THE SETTLINGS

THEY HAD ADOPTED BASED ON

RECOMMENDATION MADE BY THE

ASSISTANTS.

WE TRIED HARD WITH NUDGES LIKE

THE ONE YOU SEE HERE.

THE NUDGES ARE VERY EFFECTIVE.

WHEN IT COMES TO GETTING TEAM

CHANGE THEIR SETTINGSs, WE

HAVE DATA THAT SHOWS THOSE TYPES

OF NUDGES WORK VERY WELL.

HERE IS WHAT WE 2000.

WE FOUND AMONG AMONG THE

RECOMMENDATION MADE FOR THE

MOBILE APPS ABOUT 3/4 OF THE

RECOMMENDATIONS WERE ADOPTED BY

USERS AND WE ALSO FOUND THAT

EVEN AFTER THEY ADOPTED THESE
RECOMMENDATIONS AND MODIFIED
THEIR SETTINGS BASED ON THE
RECOMMENDATION, EVEN THOUGH WE
WERE TRYING VERY HARD TO GET
THEM TO RESIST THE SETTINGS THEY
WOULD NOT CHANGE THEM.
THAT MEANS IN THIS CASE, ABOUT
5.6% OF THOSE RECOMMENDATIONS
WERE LATER MODIFIED DESPITE
NUDGES THAT WE'RE SENDING THEM
TO REVISIT AND RETHINK THEIR
SETTINGS.
HOW DO YOU KNOW THEY MIGHT SAY
PERHAPS THEY WERE JUST LAZY AND
I GO IN ORDER YOUR SETTINGS.
WE HAD INTENTIONALLY COME UP
WITH RECOMMENDATIONS WHERE WE
WERE IGNORING A NUMBER OF OTHER
SETTINGS SO THEY COVERED
SETTINGS THAT WE HAD NOT COVERED
IN RECOMMENDATIONS AND THOSE
SETTINGS USERS WERE MODIFYING SO

WE KNOW THAT THEY WERE TRULY ENGAGED SO THIS SUGGESTS TO US THAT THESE RECOMMENDATIONS ARE PRETTY CHOSE TO HOW PEOPLE MEME FEEL ABOUT THESE ISSUES AND WE FEEL THIS IS THE WAY TO GO FOR MOBILE APPS.

THE QUESTION IS CAN WE GO ONE STEP FURTHER AND CAN YOU GENERALIZE THIS TO IOT SO WE STARTED TO WORK IN THIS AREA.

THE VISION IS HERE IS THAT YOU WOULD EXTEND THIS TO DEAL WITH SMART SPACES.

SO WHAT WE'RE DOING IS BUILDING AN INFRASTRUCTURE WHERE OWNERS OF DIFFERENT RESOURCES THAT WILL BE USING DIFFERENT ASPECTS OF BEHAVIOR, CAMERAS, PRESENCE SENSORS AND LOCATORS AND THE LIKE, THE RESOURCES HAVE TO BE DEFINED IN THE REGISTER BIT OWNERS, THE PEOPLE THAT OWN

THESE VARIOUS RESOURCE EVERS.
WE KNOW NOW ENTER A ROOM LIKE
THIS THERE ARE A NUMBER OF
DIFFERENT PEOPLE THAT COULD
DEPLOY DIFFERENT RESOURCES
ALREADY TODAY THAT COLLECT SOME
OF YOUR INFORMATION.
FOR INSTANCE IT COULD BE THE
CASE, I HOPE IT'S NOT THE CASE
BY THE COULD BE THE CASE THAT
THE WiFi ROUTERS IN THIS ROOM
PERHAPS COLLECT YOUR
INFORMATION.
THESE WiFi ROUTERS ARE NOT
OWNED BY THE PEOPLE THAT OPERATE
A BUILDING.
PERHAPS THEY'RE OWNED BY FTC OR
A THIRD PARTY, AND ON THE OTHER
HAND THE HVAC SYSTEM IN THIS
BUILDING MAY BE OWNED BY A
DIFFERENT ENTITY AND THEY MAY BE
COLLECTING INFORMATION TOO.
SO THE OWNERS OF THESE RESOURCES

SHOULD BE ABLE TO SIMPLY DECLARE
WHERE THESE RESOURCES ARE
DEPLOYED AND WHAT INFORMATION
THESE RESOURCES COLLECT, AND ALL
OF THE OTHER SOURCES AND
ATTRIBUTES THAT YOU WANT TO SEE
IN A POLICY.
SO WE'RE DEVELOPING AN
INFRASTRUCTURE WHERE, THROUGH A
SERIES OF MEN USE PEOPLE CAN
SPECIFY DIFFERENT ELEMENTS OF
THEIR RESOURCES WITHOUT
REQUIRING THEM TO DO ANY
PROGRAMMING AND LOOKING AT WHAT
IT TAKES TO TURN THESE -- THIS
INFORMATION INTO MACHINERY TO
PRIVACY POLICIES.
THE IDEA IS THAT USERS THEN,
WHERE THEIR PERSONALIZED PRIVACY
ASSISTANTS WOULD BE ABLE TO
BETTER SPACE, DISCOVER SOURCES.
AND THEIR ASSISTANTS WOULD
DETERMINE BASED ON THEIR

EXPECTATION AND PREACHERSES
WHAT, IF ANYTHING, THEY NEED TO
BE WARNED ABOUT OR INFORMED
ABOUT AND IF THERE HAPPENS TO BE
SETTLINGS, IN AN IDEAL WORLD
THEY WOULD LIKE THE ASSISTANTS
TO CONFIGURE THESE SETTINGS AND
WE'RE NOT HERE YET AND THAT IS
WHAT WE'RE AIMING FOR AND THIS
IS HOW THIS IS HOPEFULLY GOING
TO WORK ONE TAKE AND LET ME
QUICKLY TRY TO RECAP AND MAKE
CONNECTIONS WITH PUBLIC POLICY
IN THIS SPACE.
SO WE TRULY BELIEVE THIS
APPROACH TO EFFECTIVELY
LEVERAGING MACHINE, BUILDING
PERSONALIZED MODELS OF PEOPLE'S
PRIVACY EXPECTATION IS ONE WAY
OF MAKING NOTICE AND CHOICE
PRACTICAL.
RIGHT?
TODAY THE NUMBER OF SYSTEMS THAT

YOU'RE ENCOUNTERING IN IOT

CONTEXT IS JUST WAY TOO GREAT

FOR ANYONE TO IMAGINE THAT USERS

ARE GOING TO BE ABLE TO READ

POLICIES OR CONFIGURE SETTINGS.

THERE'S REALTY A NEED TO HELP

USERS AND TO DO SO BY NUMBER ONE

BUILDING MODELS OF WHAT THEY

CARE ABOUT, HOW THEY FEEL ABOUT

DIFFERENT ISSUES AND TRY TO

ALLEVIATE A BURDEN IN THAT

CONTEXT AND ALSO MAKE IT MATCH

EASIER FOR THE OWNERS SO

PARTICIPATE WITH THE

INFRASTRUCTURE.

SO AS IT WAS POINTED OUT IN THE

FIRST PRESENTATION ON THIS

PANEL.

ONE OF THE CHALLENGES OF IOT IS

A DIVERSITY OF PLAYERS.

IF YOU THINK ABOUT THE WAY YOU

INTERFACE WITH INTERNAL, MOST OF

YOUR DECISIONS ARE MADE BY THE

BROWSER AND IT'S SUFFICIENT TO
USE YOUR BROWSER.
ON THE MOBILE WEB, THE CELL
PHONE MEDIA OR ANDROID AND SO
IT'S SUFFICIENT TO KEFERG
SETTINGS AT THAT LEVEL NIOT IT'S
A DIFFERENT STORY WHERE YOU YOU
HAVE A NUMBER OF PLAYERS THAT
CONTRIBUTE DIFFERENT ELEMENTS
AND MANY ENTITIES DON'T HAVE THE
SOPHISTICATION THAT GOOGLE OR
FACEBOOK MAY HAVE AND WE NEED TO
MOVE FORWARDS AN OPEN
ENVIRONMENT WITH OPEN API AND
WHERE EFFECTIVELY PEOPLE WILL
EXPOSE SETTINGS THAT WILL ENABLE
ONE THROUGH PERSONALIZED PRIVACY
ASSISTANTS OR EQUIVALENT
TECHNOLOGY TO EFFECTIVELY
CONFIGURE MANY SETTINGS ON
BEHALF OF THE USER AND SO THAT'S
WHERE YOUR VISION PLAYS.
>> YOU CAN THINK OF TWO WAYS OF

DEPLOYING THE ASSISTANT

TECHNOLOGY.

ONE IS TO EFFECTIVELY ALLOW

COMPANIES LIKE GOOGLE OR

FACEBOOK, EACH ONE OF THEM

POTENTIALLY DEVELOP ITS OWN

PRIVACY ASSISTANT, BUILDING

MODELS OF USERS, AND YOU CAN

IMAGINE POTENTIAL CONFLICTS OF

INTEREST WHEN IT COMES TO THIS

AND THIS WOULD HAVE TO COME UP

WITH STRONG GUARANTEES OR YOU

CAN IMAGINE A MORE A BENEFITS

EFFORT WHERE YOU SAY AFTER ALL

THERE ARE INTERESTING

CORRELATIONS BETWEEN THE WAY

THAT YOU FEEL ABOUT YOUR

SETTLINGS WITH MOBILE APPS WHEN

IT COMES TO SHARING INFORMATION

AND YOUR SETTINGS ON FACEBOOK ON

YOUR BROIRS SO SNOWED OF ASKING

YOU THE QUESTIONS, YOU NEED ONE

OF THESE ENVIRONMENTS TO

DETERMINE WHAT YOUR POLICIES
ARE, HOW ABOUT ASKING THESE
QUESTIONS JUST ONCE AND THEN
USING A PERSONALIZED PRIVACY
ASSISTANT THAT CUTS ACROSS THE
DIFFERENT ENVIRONMENTS TO
CONFIGURE MANY OF SYMPATHIES
SETTINGS ON YOUR BEHALF.
IT'S NOT IMAIRN TEED THAT THE
API WILL BE MADE OPEN.
THEY ARE NOT.
>> THEY ARE VERY MUCH A PART OF
THE STRATEGY SOME OF THE THESE
LARGER ENTITIES HAVE WHEN IT
COMES TO BUILDING THEIR SYSTEMS
BUT WOULD LIKE TO EFFECTIVELY
BUILD ANEST TO CONVINCING THESE
LARGER PLAYERS THAT THEY WOULD
BENEFIT FROM OPENING THE API AND
PERHAPS PEOPLE WOULD ASK ME
QUESTIONS LATER ON SO I CAN SAY
MORE ABOUT THIS BUT I'M AFRAID I
HAVE RUN OUT OF TIME SO THANK

YOU VERY MUCH.

>>

[APPLAUSE]

>> WE WILL CONCLUDE TODAY WITH
OUR FINAL DISCUSSION OF THE DAY.
SO UNLIKE PREVIOUS SESSIONS THAT
HAVE FOCUSED MOSTLY ON PRIVACY,
THIS SESSION FOCUSED ON SECURITY
AND USABILITY AS IT RELATES TO
PRIVACY.
SO SARTHAK GROVER DISCUSSED
SECURITY ISSUES RELATED TO THE
IOT DEVICES AND HOW THEY AFFECT
PRIVACY IN THE HOME.
VITALY SHMATIKOV PRESENTED ON AD
LIBRARIES AND HOW THE LACK OF
TAILORED SECURITY CONTROLS IN
SOME CONTEXT COULD RESULT IN
DISCLOSURE OF USERS' INFORMATION
THROUGH SHARED EXTERNAL STORAGE.
FOR USABILITY FLORIAN SCHAUB
SHARED ABOUT A LINE OF RESEARCH
GOING ON AROUND USING MACHINE

LEARNING, AND CROWD SOURCING AND OTHER METHODS TO MAKE PRIVACY POLICIES MORE USABLE AND FOR CONSUMERS FOR BUSINESSES AS WELL AS MAYBE FOR REGULATORS, FINALLY NORMAN SADEH PRESENTED NEW WAYS TO UNDERSTAND AND MANAGE USERS' PRIVACY EXPECTATIONS THROUGH PERSONAL PRIVACY ASSISTANTS.

SO OVERALL THIS SESSION HAS PROVIDED SOME NEW VIEWS INTO DIFFERENT STRANDS OF PRIVACY RESEARCH TO CONSIDER.

AND WITH THAT, ALL OF THOSE WILL ADD TO THE POLICY CONVERSATION HERE.

I WANT TO WELCOME GEOFFREY MANNE, THE EXECUTIVE DIRECTOR OF THE INTERNATIONAL CENTER FOR LAW AND ECONOMICS AS WELL AS ITS FOUNDER AND DAVI OTTENHEIMER WHO HOLDS MANY HATS IN THE BUSINESS COMMUNITY INCLUDING ONE ON BIG

DATA SECURITY.
GEOFFREY AND DAVI WILL PROVIDE
THOUGHTS ON THIS SESSION AS IT
RELATES TO PRIVACY FOR A FEW
MINUTES EACH AND WE WILL START
THERE.
SO GIVE?
GEOFF?
>> I THOUGHT THE PAPERS
PRESENTED INTERESTING THINGS AND
AS DID THE PAPERS THROUGHOUT THE
DAY AND SINCE THIS IS THE LAST
SEX AND I HAVE YOU HEAR I'M
GOING TO TALK A LITTLE MORE
BROADLY AT FIRST THAN JUST ABOUT
THE PAPERS TODAY BUT IN A WAY
THAT IS CONSISTENT WITH WHAT
AARYN WAS SAYING WHICH IS TO SAY
THAT THE PAPERS ARE INTERESTING,
THERE'S REALLY IMPORTANT STUFF
HERE, BUT AS IS SO OFTEN THE
CASE, THE PROBLEM IS DERIVING
THE APPROPRIATE POLICY

IMPLICATIONS FROM IT.
ONE OF THE THINGS I WOULD SAY IS
THAT IT'S A LITTLE BIT
UNFORTUNATE, WE DON'T HAVE MORE
ECONOMISTS AND ENGINEERS TALKING
TO EACH OTHER.
AS YOU MIGHT HAVE GATHERED FROM
THE LAST PANEL, AN ECONOMIST
WILL TELL YOU THAT MERELY
IDENTIFYING A PROBLEM ISN'T A
SUFFICIENT BASIS FOR REGULATING
TO SOLVE IT, NOR DOES THE
EXISTENCE OF A POSSIBLE SOLUTION
MEAN THAT THAT SOLUTION SHOULD
BE MANDATED.
AND YOU REALLY NEED TO IDENTIFY
REAL HARMS RATHER THAN JUST
INFORMING THEM AS JAMES COOPER
POINTED OUT EARLIER AND WE NEED
TO GIVE THOUGHT TO SELF HELP AND
REPUTATION AND COMPETITION AS
SOLUTIONS BEFORE WE START TO
INTERVENE.

IT IS CERTAINLY SOMETHING IN THE
NATURE OF A CONFERENCE LIKE THIS
AND FOR THAT MATTER OF THE KINDS
OF PAPERS THAT PEOPLE ARE
WRITING BECAUSE JOURNALs DON'T
PUBLISH PAPERS SAYING NOTHING IS
WRONG.
>> THEY PUBLISH PAPERS SAYING
THERE'S A PROBLEM AND PERHAPS
SUGGESTING SOLUTIONS TO THEM.
SO WE TALKED ALL DAY ABOUT
PRIVACY RISK, BIAS CEASE AND
DATA, BAD OUTCOMES AND PROBLEMS
BUT WE HAVEN'T TALKED ABOUT
BENEFICIAL USES THAT THESE
THINGS MAY ENABLE.
SO DERIVING POLICY PRESCRIPTIONS
FROM THESE SORT OF LOPSIDED
DISCUSSIONS IS REALLY PERILOUS.
NOW THERE'S ANOTHER ADDITIONAL
PROBLEM THAT WE HAVE IN THIS
FORUM AS WELL WHICH IS THAT THE
FTC HAS A TENDENCY TO FIND

JUSTIFICATION FOR ENFORCEMENT DECISIONS IN THINGS MENTIONED AT WORKSHOPS JUST LIKE THESE SO THAT MAKES IT DOUBLY RISKING TO BE TALKING EVEN ABOUT THESE THINGS WITHOUT POINTING OUT THAT THERE ARE IMPORTANT BENEFITS HERE AND THAT THE COSTS MAY NOT BE AS DRAMATIC AS IT SEEMS BECAUSE WE'RE PRESENTING THE PAPERS DESCRIBING THEM.

THINK ABOUT THE POTENTIAL VULNERABILITIES THAT WE TALKED ABOUT ON THIS PANEL: THE QUESTION TO ME BECOMES: SHOULD THEY LEAVE THE FTC TO ANY FIND OF ENFORCEMENT IF COMPANIES DON'T ENGAGE IN THE TYPE OF SECURITY RECOMMENDED IN SOME PLACES OR ANY SECURITY AT ALL AND AGAIN THIS IS AN FTC WORKSHOP SO COULD YOU BELIEVERS ARE GOING TO HAVE TO WONDER IF

THEIR COMPANIES ARE NOW ON

NOTICE, AND IF THE VERY

SELECTION OF PAPERS HERE

INDICATES ANYTHING ABILITY THE

FTC'S ENFORCEMENT AGENDA.

HAVING HAD A POSSIBLE

VULNERABILITY AND ACTING

UNFAIRLY UNDER SECTION 5 ARE NOT

THE SAME THING AND BY THE WAY

THAT'S ESSENTIALLY THE HOLDING

IN THE AOJ'S DECISION AGAINST

THE FTC IN THE LAB MD CASE.

ALSO IN TERMS OF THE GIEBILITY

DESIRABILITY OF ENFORCEMENT I

THINK IT'S IMPORTANT TO NOTE

THAT A COUPLE OF PAPERS IN THIS

SESSION AND ELSEWHERE THROUGHOUT

THE DAY HAVE SUGGESTED THAT

EITHER SELF-HELP IS OR CAN BE

WORKING.

NORM MON'S PAPER MOST OBVIOUSLY

AND IMMEDIATELY SUGGESTED A

VERSION OF THAT.

OR THAT, DESPITE THE POTENTIALIALITY OF ALL OF THESE PROBLEMS, SOMETHING IS ACTUALLY PREVENTING THESE VULNERABILITIES FROM BEING EXPLOITED.

SELF HELP HAS DIRECT LEGAL IMPLICATIONS SAY FOR A DECEPTION CLAIM WHERE IT MATTERS TO IT'S AVAILABLE BUT BOTH SELF HELP AND THE LIMITED EXPLOITATION OF RISK ARE IMPORTANT IN THE ECONOMIC CALCULUS OF THE DESIRABILITY OF ENFORCEMENT.

SO I WANT TO END QUICKLY BY SAYING -- I HAVE MORE SPECIFIC QUESTIONS AND COMMENTS WE DISCUSSED BUT OVERALL I WOULD LIKE TO SAY THAT LAST POINT IS AN AREA WHERE WE'RE LACKING IN RESEARCH AND I WOULD LIKE TO TO SEE MORE RESEARCH ON THE IMPLICATIONS OF THE AVAILABILITY OF SELF HELP AND WHAT ARE THE

INCENTIVES FOR CONSUMERS

THEMSELVES?

WE SPEND ALL OF OUR TIME TALKING

ABOUT THE INCENTIVES OF FIRMS

AND THE IMPLICATIONS OF LEGAL

LIABILITY ON FIRMS BUT WHAT

ABOUT THE CONSUMERS THEMSELVES?

WHAT ABOUT SELF HELP AND HOW

DOES AND SHOULD THE FTC TAKE

ACCOUNT OF THOSE?

>> DAVI?

>> WELL I FEEL LIKE SOMEBODY HAS

GIVEN ME A BIG BASKET OF BALLS

TO JUGGLE HERE AT THE END OF THE

DAY AND I WILL TRY TO MAKE SENSE

OF IT ALL.

TEEING OFF WHAT GEOFF JUST SAID

THERE ARE IDEAS THAT THERE ARE

EXPERIENCES WE CAN HAVE AND

THINGS WE CAN DISCOVER THROUGH

HARD SCIENCE IS A FAIR SPLIT AND

I WILL ATTRIBUTE IT TO THE FOUR

TALKS.

I THINK THAT GOES BACK TO THE

QUESTION SHOULD YOU STUDY

COMPUTER SCIENCE OR SOCIAL

SCIENCE?

SHOULD YOU HAVEN APPLIED

APPROACH TO RISK OR SHOULD YOU

HAVE AN ACADEMIC APPROACH AND A

LOT OF TIMES PEOPLE PEOPLE

FORGET THERE'S SOMETHING IN THE

MIDDLE SO IT WAS INTERESTING TO

HERE THE FIRST SPEAKER TALK

ABOUT ONE END OF THE SPECTRUM

WHICH IS UNIT TESTS OF THESE IOT

DEVICES AND THEN THE SECOND

SPEAKER TOOK US THROUGH AN

INTEGRATION TEST SCENARIO WHERE

WHAT ARE THE DEVICE LIKE IN THE

WILD AND LET'S LOOK HOW THEY'RE

USED BY PEOPLE AND THE ECONOMIC

AND THE SOCIAL SCIENCE OF AND

THOSE ARE PARTS OF THE SPECTRUM

AND THE THIRD AND FOURTH

SPEAKERS BROUGHT IN THE MIDDLE

GROUND WHERE YOU HAVE SOMEBODY

SAYING WE CAN USE THIS EXERCISE

TO HELP PEOPLE MAKE SMALL

RATIONAL DECISIONS SO YOU REDUCE

THE DECISIONS AND CRITERIA SO

PEOPLE CAN CHOOSE FROM SOMETHING

RELATION STICK SO YOU'RE NOT

FORCING PEOPLE TO MAKE BIG

ANALYTIC ANALYSIS AND IT'S SMALL

AND THAT'S THE TWO ENDS THAT I

SEE AND THEN EVEN MORE

INTERESTINGLY HAS A SHARED MODEL

WHERE NOT ONLY ARE YOU MAKING

THINGS EASIER TO DECIDE ACCURACY

AND CHOICE BUT YOU'RE

ENCOURAGING

ENCOURAGING AND NUDGING PEOPLE

AND BRINGING AN ECONOMIC MODEL

TOWARDS THE MIDDLE TO DECISIONS

WITH NUDGES AND THAT'S HOW I SEE

THE FOUR PUT TOGETHER AND I HAVE

A TON OF QUESTIONS FOR ALL OF

THE SPEAKERS BUT WE DON'T HAVE

THANK MUCH TIME.

>> SO I WANTED TO ASK, SINCE
WE'RE RUNNING OUT OF TIME I
WANTED TO ASK A GENERAL QUESTION
ACROSS ALL PRESENTERS, IF
THERE'S ONE POLICY MESSAGE THAT
YOU THINK YOUR RESEARCH IS
NEONATALLING IN AS YOU DISCUSSED
IN YOUR PRESENTATIONS BUT IS
LACKING IN TECHNICAL MEASURES
THAT WOULD ACTUALLY HELP YOU
IMPLEMENT THE POLICY GOAL THAT
YOU WOULD LIKE TO SEE WHAT ARE
THOSE SHORTCOMINGS AND HOW WOULD
YOU LIKE THOSE SHORTCOMINGS
ADDRESSED?
AND IT'S OPEN TO ANY OF THE
PRESENTERS.

>> IT'S A TOUGH ONE.
CLEARLY ONE HAS TO BE REALISTIC
ABOUT WHAT CAN BE DONE AND HOW
MUCH ROOM FOR MANEUVER I GUESS
THE FTC HAS IN THIS SPACE BUT I

SUSPECT THAT THE FTC CAN PLAY A
ROLE IN BRINGING TOGETHER KEY
STAKEHOLDERS AND ENCOURAGING
DIALOGUES AND SO FOR INSTANCE
THE ISSUE THAT I WAS ALLUDING TO
AT THE END OF THE MY TALK IN
TERMS OF OPENING API'S CLEARLY
THIS WOULD NEVER BE SOMETHING
ONE WOULD BE ABLE TO MANDATE BUT
PERHAPS EFFORTS CAN BE
ENCOURAGED BY BRINGING TOGETHER
KEY STAKEHOLDERS.

AT THE END OF THE DAY WHEN
PRIVACY IS PRESENTED THE RIGHT
WAY AND WHEN PEOPLE ARE LOOKING
AT THIS RATIONALLY EVERYONE CAN
BENEFIT FROM BETTER PRIVACY
INCLUDING VENDORS THAT, YOU
KNOW, ARE SOMETIMES PRESENTED AS
IF THEY DIDN'T CARE ABOUT
PRIVACY.

I THINK THAT IF YOU LOOK FOR
INSTANCE AT WHAT IS HAPPENING

TODAY IN MOBILE SPACE, IT'S VERY CLEAR THAT EVERYONE HAS COME TO REALIZE THAT IS THEY DON'T WANT TO BE SEEN AS THEY DON'T CARE ABOUT PRIVACY AND THAT CREATES STRONG INCENTIVES TO THINK OF WAYS THEY HAVE BEEN APPROACHING DECISIONS IN THAT SPACE SO I THINK PERHAPS THE FTC CAN ON THE ONE HAND CONTINUE TO DO WHAT IT HAS BEEN DOING WHICH IS TO ENCOURAGE BEST PRACTICES AS IT HAS DONE FOR INSTANCE FOR MOBILE APPS AND DONE RECENTLY WHEN IT COMES TO IOT SECURITY, AND PERHAPS ALSO CONVENING MEETINGSES AND ENCOURAGING EFFORTS WHERE PEOPLE LOOK AT OPPORTUNITIES FOR PERHAPS DEVELOPING COMMON STANDARDS, NOT TRYING TO IMPOSE ANY STANDARDS AND YOU KNOW STANDARDS ARE VERY CHALLENGING AND VERY TRICKY

EFFORTS BUT TRYING TO BRING
TOGETHER KEY STOCKHOLDERS AND
GETTING -- STAKE HOLDERS AND
WHERE THEY HAVE COMMON INTEREST
AND DEVELOPING OPEN API'S.

>> I THINK TRANSPARENCY IS VERY
IMPORTANT.
BETTER UNDERSTANDING AND BETTER
DISCLOSURE OF HOW INFORMATION IS
COLLECTED AND SHARED BETWEEN
VARIOUS PLAYERS IN THE PICTURE
IS CRUCIALLY IMPORTANT.
BECAUSE WHAT WE HAVE IN MOBILE
SPACE TODAY IS OLD PERMISSION
MODELS.
THEY CAPTURE SOMETHING ABOUT THE
SECURE DEVICES AND CAPTURE
NOTHING ABOUT PRIVACY.
THERE IS A LOT OF INFORMATION
COLLECT AND SHARING AND
INFORMATION USED BETWEEN ALL
KINDS OF ARTISTS, PLATFORM
OPERATORS, AD LIBRARIES, APP

BUILDERS, ADVERTISERS, THAT
SIMPLY EXISTS OUTSIDE OF THE
EXISTING PERMISSION MODELS THAT
A LOT OF PRIVACY WORK FOCUSES ON
SO TO THE EXTENT FTC CAN HELP
SHED LIGHT ON THIS AND ASK FOR
MORE DISCLOSURE INFORMATION
PRACTICES AND INFORMATION FLOWS
IN THIS MASSIVE MOBILE ECOSYSTEM
THAT COULD BE AN EXTREMELY
USEFUL SERVICE AND IS THAT NOT
HAPPENING TODAY.
>> SO I TO TOTALLY AGREE WITH
THAT.
LIKE MAYBE THE FTC CAN -- IN
TERMS OF DEVICES AND APPS, THAT
IN NEVERTHELESS POLICIES WE
WON'T ALLOW YOU TO SELL THESE TO
OTHERS BUT IN TERMS OF
IDENTIFYING DEVICES THAT NOT
REALLY OPEN API'S AND WHO REALLY
SITS THERE AND LOOKS AT ALL OF
THIS, LIKE WHO DOES THE ANALYSIS

WHEN YOU DON'T HAVE ACCESS TO
THE CODE AND THE SOFTWARE AND
THE HARDWARE ARE BASICALLY
INTEGRATED.
I CAN'T YOU DON'T HAVE CHOICES
IN CASE YOU FEEL LIKE SOMETHING
SO WRONG.
YOU WANT TO LEAVE A PLACE IF
IT'S IS SOMEWHERE ELSE.
SO TRANSPARENCY IS THE MAIN
ISSUE AND IT SHOULD BE
ENCOURAGED BUT QUITE FRANKLY I
DON'T KNOW HOW TO GO ABOUT IT.
>> BUT BUST THINGS -- THERE'S
ALWAYS TRADEOFFS AND IT MAY NOT
SURPRISE YOU TO LEARN I WROTE A
PAPER CALLED THE COMPOSITE OF
DISCLOSURE SO I AGREE
TRANSPARENCY TENDS TO BE A GOOD
WAY OF ACHIEVING THESE THINGS
BUT IT'S NOT COSTLESS,.
AS LAUREN HAD ON THE LAST SLIDE
IF WE HAVE OPEN API WE WILL BE

EMPOWERING THE GROUPS THAT
COLLECT THIS MASSIVE AMOUNT.
NAVIGATION THROUGH OPEN API WITH
AN ENORMOUS AMOUNT OF
INFORMATION THAT CREATES PERHAPS
EVEN GREATER VULNERABILITIES
THAN THE ONES THAT WE'RE
PROTECTING AND THAT -- THERE MAY
BE OTHER EXAMPLES LIKE THAT,
TOO, SO MY QUESTION REALLY IS,
BEFORE WE SETTLE ON TRANSPARENCY
EVEN AS THE RIGHT SORORITY OF
OPTIMAL SOLUTION HERE WE SHOULD
BE AWARE THAT THERE ARE COSTS TO
THAT AS WELL, AND THAT AGAIN
THAT POTENTIALLY WE'RE CREATING
MORE RISKS THAN WE'RE SOLVING.
>> I PUT IT AS TRANSPARENCY TO
WHOM?
YOU'RE BUILDING A TRUST
RELATIONSHIP SO IT'S
TRANSPARENCY TO SOMEBODY THAT
YOU ESSENTIALLY TRUST GLORIFY

YOU THE RIGHT ANSWER GIVEN THAT
THEY HAVE THE INFORMATION SO I
HAVE GONE AUDITS OVER 20 YEARS
AND I CAN TELL YOU JUST BEING
ABLE TO SEE INTO SOMETHING
DOESN'T MEAN YOU'RE IN A
POSITION TO MAKE A DECISION ON
IT.
WHICH IS SORT OF WHAT THE
PRESENTATIONS WERE ABOUT TO SOME
DEGREE WE GIVE PEOPLE IT HAD
INFORMATION, THE PEOPLE AREN'T
IN A POSITION TO DIGEST IT
BECAUSE THEY DON'T HAVE THE
ANALYTIC CAPABILITY TOTE THEY'RE
GIVEN THE INFORMATION SO IF YOU
TAKE SORT OF THE UNIT TEST YOU
CAN SAY THAT IS INADEQUATE
BECAUSE YOU HAVE COMPLIANCE
CHECKLIST AND IF YOU TAKE THE
ENVIRONMENTAL OR INTEGRATION
TEST YOU CAN SAY THAT IS NOT
FAIR BECAUSE THAT'S NOT A

TYPICAL USE CASE SO SOMEWHERE IN
THE MIDDLE IS PROPER USE OF
DEVICE PREPARED FOR USE CASE AND
THAT'S I THINK A GOOD FIT.

>> SO I THINK CONCERNING
TRANSPARENCY AN INTERESTING
POINT TO THINK ABOUT IS THAT THE
PRIVACY POLICIES THAT WE HAVE
RIGHT NOW, THEY'RE NOT WRITTEN
FOR USERS AND THEY'RE NOT MEANT
230 PROVIDE TRANSPARENCY FOR
USERS AND WE NEED TO REALIZE
THIS AND I THINK THIS NEEDS TORE
CLEARER IN REGULATION AS WELL
THAT IF WE WANT TO INFORM USERS
AND CREATE TRANSPARENCY THEN WE
NEED TO COME UP WITH USER
NOTICES THAT ARE MADE FOR USERS
AND THAT COULD INCLUDE REQUIRING
USER EVALUATION OF THOSE
NOTICES, ARE THEY ACTUALLY
EFFECTIVE AT COMMUNICATING WHAT
THEY'RE SUPPOSED TO COMMUNICATE

AND WE HAVE BEEN DOING A LOT OF
THESE STUDIES AND WE FIND MOST
NOTICES ARE NOT EFFECTIVE.
AND IT'S REALLY HARD TO DESIGN
EFFECTIVE NOTICE.
>> HERE IS AN INTERESTING
COUNTERPOINT, THE MORE
INFORMATION THAT BECOMES
AVAILABLE, THE MORE BEHAVIOR
CHANGES SO IF YOU ACTUALLY -- I
COULD SHOW YOU EXPLOITS FOR
EXAMPLE TWO YEAR MODEL THAT
SHOWS AS YOU GET THIS IN
POSITION WHERE YOUR MACHINE
ALGORITHMS ARE WORKING AND YOU
GET THE ANSWERS THAT YOU WOULD
THE POLICY LESS CHANGE SO YOU
CAN'T SEE THEM ANYMORE SO THE
TRANSPARENCY HAS TO BE IN
CONCERT WITH THE RIGHT MODEL
WHERE PEOPLE WANT IT TO BE SHOWN
IN THE WAY THAT IS COMFORTABLE
FOR THEM OTHERWISE THEY ADAPT

AND YOUR TRANSPARENCY BACK
FIRES.
>> NORM AROUND DID YOU WANT TO
ADDRESS THE TRANCE GLAIRNS I
WOULD LIKE TO RESPOND TO THE
LAST COMMENT.
SO I THINK IT'S CLEAR THAT
PRIVACY IS AN ARMS RACE.
I THINK THAT I WORK TOGETHER
WITH FLORIAN ON THE POLICY THAT
HE DESCRIBED BUT THE DAY THAT
SITE OPERATORS START MODIFYING
THEIR POLICY BASED ON OUR
TECHNOLOGY, BECAUSE OF THE
SUCCESS OF OUR TECHNOLOGY WILL
BE A VERY GOOD DAY.
WE'RE NOT QUITE THERE YET IF
THAT DAY HAPPENS WE WILL HAVE
THE ABILITY TO PROBABLY IDENTIFY
THAT AND THAT MIGHT POTENTIALLY
BE SOMETHING THAT THE FTC WILL
BE INTERESTED IN, AND WHETHER
THEY WOULD BE ABLE TO DO MUCH

ABOUT IT OR NOT, I'M NOT
SUFFICIENTLY VERSED INTO THE
LEGAL RAMIFICATIONS OF THAT BUT
I SUSPECT THAT IT WOULD HAVE
SOMETHING TO SAY IF YOU CAN
ESTABLISH EFFECTIVELY A PATTERN
WHERE ONCE YOU ARE EFFECTIVE
LIVE ABLE TO CAPTURE A PRACTICES
THAT PROSECUTE NOT PUTTING THE
COMPANIES IN A GOOD LIGHT AND A
START MODIFYING THE WAY THEY ARE
INTERPRETING THE TEXT AND I
SUSPECT SOMETHING COULD
POTENTIALLY BE DONE.
>> AND IT'S ALSO A MATCH THAT I
IT TWO GOT OTHER WAY SO KEEPS
IMPROVE THE LANGUAGE TO BE
BETTER PRESENTED BY THESE
INFORMATION MECHANISMS AND WE
HAVE CONVERSATIONS WITH MANY
DIFFERENT COMPANIES THAT SAY
THEY WOULD ACTUALLY WELCOME
HAVING SUCH TECHNOLOGY OUT THERE

BECAUSE THEY DO INVEST A LOT OF
MONEY AND TIME IN HAVING PRIVACY
POLICIES THAT ARE DESCRIPTIVE
BUT IT'S BASICALLY IN VEIN
BECAUSE THIS INFORMATION IS NOT
USED AND THIS IS THE CASE.
>> SO I THINK THIS COULD GO BACK
WAYS.
>> THE PRIMARY REASON FOR
UNINTELLIGENCABILITY FOR
EXISTING POOLSES IS IS THE LEGAL
RISK, IS -- AND FOR THAT METER,
EVEN REGULATORY ENFORCEMENTS
ASSOCIATION.
>> IN WE DON'T HAVE DISCLOSURE
THAT INFORMATION THE USERS THEN
TO ME WE HAVE IDENTIFIED A
IMPORTANT DISCONNECT BETWEEN HOW
WE'RE REGULATING AND THE POWER
OF USERS WHICH GOES TO THE POINT
I WAS MAKING BEFORE WHICH IS
THAT I REALLY LIKE WHAT YOU WERE
DESCRIBING, THE SORT OF APP THAT

YOU GUYS CREATED AND IT SEEMS TO
ME LIKE IT HAS AMAZING POTENTIAL
AND ONCE WE HAVE SOMETHING LIKE
THAT THINK OF WHAT THAT DOES TO
THE NEED FOR ADDITIONAL FORMS OF
REGULATION YOU HAVE DONE A GOOD
JOB OF GIVING USERS WHAT THEY
WANT AND BECAUSE USERS ARE SO
LET GENIUS AND TYPES OF DATA ARE
HETEROGENEOUS AND I THINK ONYOUR PAPER THERE'S A BIG
DIFFERENCE BETWEEN AN E-MAIL
ADDRESS BEING ACCESSIBLE AND THE
CONTENT OF A COMMUNICATION EVEN
WITH A COMPUTER DEVICE.
>> A REAL PROBLEM WITH
OVERGENERAL AND THIS MAY BE
REFLECT THE IN THE BAD PRIVACY
POLICIES A PROBLEM WITH SORT OF
AN OVERGENERAL RESPONSE LIKE A
NETWORK LEVEL RESPONSE TO THE
PROBLEM YOU WERE IDENTIFYING IS
THAT -- WELL I DON'T KNOW,
ENOUGH ABOUT.ENGINEERING BUT AT

FIRST CUT I WOULD SAY IT DOESN'T
DIFFERENT, IT JUST IMPOSE'S
SINGLE POLICY ON EVERYONE
REGARDLESS.
AND THAT IS REALLY UNLIKELY TO
BE THE RIGHT OUTCOME.
BUT IS THAT A PROBLEM WITH YOU
KNOW SORT OF THE MORE BLOUNT --
RELATIVELY BLUNT POLICY TOOLS
THAT WE HAVE, SO YOU KNOW AGAIN
I THINK THERE'S REAL VALUE IN
EMPOWERING EUTZERS SLOAFNTION AT
LEADS TO A REDUCTION IN THE
INCENTIVE OF THESE MORE BLUNT
TOOLS TO COME N.
>> SO WE HAVE ABOUT 45 SECONDS
LEFT.
I WANTED TO ASK IF YOU HAD THE
IDEAL PRIVACY AGENDA IN YOUR
RESEARCH, WHAT WOULD IT BE IN
ONE OR TWO SENTENCES GOING
FORWARD?
>> I THINK I HAVE OUTLINED OUR

AGENDA AND THERE WERE THREE
PRESENTATIONS AND I STRONGLY
BELIEVE IN THE PRIVACY
ASSISTANTS.
IT'S CLEARLY NOT SOMETHING WHERE
WE ARE ENTIRELY THERE YET BUT WE
HAVE PROM PROMISING RESULTS IF.
IF I COULD TAKE ANOTHER
30-SECONDS --
>> NO.
SORRY.
>> ALL RIGHT.
BUT THANK YOU THOUGH.
>> OK.
>> SO I THINK WHAT IS ALSO
IMPORTANT, WHAT WE'RE STARTING
TO LOOK AT IS PROVIDING
INFORMATION AND INTEGRATING
THE -- THESE DIALOGUES INTO THE
USERS INTO ACTION FLOW.
SO RATHER THAN HAVING A PRIVACY
NOTICE, A PRIVACY POLICIES
SOMEWHERE ELSE, WHEN THE USERS

INTERACTS WITH IT MAKE IT PART
OF THE INTERACTION.
THE MOBILE PLATFORM DEVELOPERS
ARE DOING A GOOD JOB DOING THIS
ALREADY, OR STARTING TO DO THIS
ALREADY.
YOU HAVE THOSE JUST IN TIME
DIALOGUES THAT POP UP AND THEY
DON'T DISRUPT THE INTERACTION
FLOW.
THEY HELP IT AND ENCOURAGE THE
APP DEVELOPERS TO BUILD DIALOGUE
AROUND IT THAT TELL YOU WHY THIS
NOTIFICATION IS GOING TO POP UP
AND WHY THEY WANTED YOUR
LOCATION.
THAT'S GREAT AND I THINK IT'S A
GOOD DIRECTION AND WE ARE DOING
INTERESTING RESEARCH TO THE
EXTENT OF THAT AND OTHER THINGS.
>> AND WE'RE NOT BIAS GRD I WILL
STOP YOU THERE.
ENCOURAGE THE AUDIENCE TO ASK

AFTER THAT BUT I WANTED TO CON
COLLIDE BY -- OH, THERE YOU R
OK.
SO THE FTC'S NEW CHIEF
TECHNOLOGIST STARTED ON MONDAY,
AND SO I WANTED TO WELCOME
LORRIE CRANOR FROM THE EXPRFT WE
ALSO THANK CARNEGIE MELLON FOR
ALLOWING HER TIME ON LEAVE FOR
HER TO BE HERE WITH US.
>> THANK YOU. I WILL KEEP MY
REMARKS BRIEF SINCE WE'RE OVER
TIME.
FIRST OF ALL I WANTED TO THANK
ALL OF THE FTC STAFF WHO DID
SUCH A WONDERFUL JOB ORGANIZING
THIS.
CAN WE GIVE THEM A BIG ROUND OF
APPLAUSE:
[APPLAUSE]
>> YEAH, THIS IS MY FOURTH DAY
SO I HAD NOTHING TO DO WITH IT
BUT THESE GUYS DID A GREAT JOB.

I WANTED TO THANK YOU ALL FOR
COMING AND FOR PARTICIPATING.
A FEW NOTES ON SOME THINGS I
HEARD THROUGHOUT THE DAY, TSA IT
WAS A LOT TO ABSORB AND TRYING
TO SYNTHESIZE WHAT I HEARD, SO I
THINK SOME OF THE KEY AREAS THAT
I HEARD -- THERE'S A LOT OF
REALLY INTERESTING, EMPIRICAL
RESEARCH THAT IS BEING DONE.
AND SOME OF THE AREAS THAT IT'S
BEING DONE IN THAT WE HEARD
ABOUT.
WE HEARD ABOUT SURVEY AND
INTERVIEW RESEARCH, ABOUT WHAT
CONSUMERS UNDERSTAND, AND
ESPECIALLY WHAT THEY EXPECT AND
WHAT THEY DESIRE.
WE ALSO SAW THAT SOME OF THIS
RESEARCH IS THEN BEING USED TO
FIND WAYS TO ACTUALLY ASSIST
CONSUMERS FIGURING OUTWEIGHS TO
REDUCE THE NUMBER OF NOTICES

THAT THEY NEED 20 SEE AND
CONFIGURE THEIR SETTINGS
AUTOMATICALLY.
A QUESTION THAT CAME UP IN
ALMOST EVERY PANEL I THINK WAS A
QUESTION ABOUT HOW WE CAN MAKE
TRANSPARENCY IN NOTICE AND
CHOICE MORE EFFECTIVE.
WE HEARD OVER AND OVER AGAIN HOW
INEFFECTIVE IT SEEMED TO BE AND
WE HEARD SOME WAYS FORWARD, SOME
PATHS TO MAYBE MAKING IT MORE
EFFECTIVE.
WE ALSO HEARD ABOUT MEASUREMENT
RESEARCH THAT LOOKED 59 A
VARIETY OF THINGS.
WE HEARD ANT MEASUREMENTS ON THE
EXTENT THAT PEOPLE ARE BEING
TRACKED AND WHAT TECHNOLOGIES
ARE TRACKING THEM.
AND WE ALSO HEARD ABOUT
STATISTICAL AND LEARNING MACHINE
RESEARCH TO UNDERSTAND HOW

ALGORITHMS IMPACT USERS AND OUR
SPEAKERS OBSERVED THAT IN ORDER
TO HAVE ALGORITHMIC TRANSPARENCY
IT'S NOT ENOUGH JUST TO KNOW
WHAT OF THE ALGORITHMS ARE
BECAUSE THAT DOESN'T REALLY TELL
US VERY MUCH.
WHAT WE NEED ARE SYSTEMS TO HELP
US INTERPRET THE RESULTS OF THE
ALGORITHMS AND HELP US
UNDERSTAND THE IMPACT MUCH THOSE
ALGORITHMS.
WE -- I SAW SOME PRESERVE THAT
BUILT MODELS AND INVESTIGATED
HAD THE IMPACTS OF DIFFERENT
APPROACHES TO PRIVACY
PROTECTION.
AND AND HELP SHED LIKE E. LIGHT
ON THE EFFECTIVENESS OF
DIFFERENT APPROACHES.
WE SAW RESEARCH TO UNDERSTAND
THE IMPACT OF INCENTIVES AND
APPROACHES 20 CYBER SECURITY.

WE ALSO SAW MANY OF THE RESEARCHERS THAT SPOKE HERE HAD DEVELOPED TOOLS THAT HAD BEEN USEFUL IN THEIR OWN RESEARCH AND MANY OF THEM HAD ACTUALLY OFFERED TO MAKE THEIR TOOLS AVAILABLE TO OTHER RESEARCHERS WHO COULD ALSO USE THEM AND I THINK THE COMMUNITY IS DEVELOPING A TREMENDOUS TOOL SET THAT SHOULD ENABLE TO LOT MORE RESEARCH TO HAPPEN GOING FORWARD.

WE ALSO HEARD FROM RESEARCH TO PARTNER WITH COMPANIES TO DO EMPIRICAL RESEARCH.

SOME PEOPLE NOTED IN ORDER TO DO THE RESEARCH THEY WANTED TO DO THEY NEEDED INFORMATION ONLY THE COMPANIES HAVE SO THERE WAS AN INVITATION TO PARTNER WITH THEM.

SO THOSE WERE KIND OF THE HIGHLIGHTS OF WHAT I HEARD

TODAY.

I'LL BE VERY INTERESTED IN

HEARING FROM ALL OF YOU ABOUT

WHAT YOU FOUND USEFUL.

WE'RE ALSO INTERESTED IN GETTING

FEEDBACK ON THIS EVENT, SHOULD

WE DO IT AGAIN?

IF SO, SHOULD WE DO IT EXACTLY

THE SAME WAY?

WHAT SHOULD WE DO DIFFERENTLY?

WE WOULD BE VIDEO INTERESTED IN

HEARING THAT FROM YOU.

ONE OF THE THINGS THAT I WOULD

LIKE TO DO WHILE I'M AT THE FTC

IS TO TRY TO BETTER BRIDGE THE

GAP BETWEEN ACADEMIC RESEARCH

AND POLICY MAKERS AND I THINK

THE PRIVACY AREA IS AN AREA

WHERE THERE'S A REAL NEED TO

INFORM POLICY MAKING WITH

RESEARCH.

AND SO AS SUCH I LOOKING FORWARD

TO TINGING THE DISCUSSIONS THAT

WE STARTED HERE THROUGH THE

YEAR.

THANK YOU. APPLAUSE.