FTC 210727 9 AM-10:15 AM

>> GOOD MORNING.
ON BEHALF OF MY COLLEAGUES AT THE FEDERAL TRADE COMMISSION, I'M HAPPY TO WELCOME YOU TO PRIVACYCON.
I'M JAMIE HINE.
I'M AN ATTORNEY IN THE DIVISION OF PRIVACY AND PROTECTION.
WE'RE HAPPY TO BRING YOU PRIVACYCON FOR THE SIXTH YEAR.
WE'RE HAPPY TO HAVE YOU JOIN THE WEBCAST.
OUR AGENDA IS AVAILABLE ON THE PRIVACYCON PAGE AND THE BIOGRAPHIES OF ALL THE PRO CENTERS TODAY.
FOLLOWING PRIVACYCON, WE'LL MAKE ALL OF THE PRESENTATIONS AVAILABLE ONLINE.
USUALLY TAKES TWO WEEKS BUT WE ARCHIVE ALL THE PRESENTATIONS TODAY.
YOU CAN GO BACK AND WATCH THEM.
WE'LL ALSO HAVE A TRANSCRIPT TO READ ALONG AND SEE ALL OF THE GREAT PRESENTATIONS AGAIN TODAY.
AFTER WHAT SEEMS LIKE A LIFETIME OF ZOOMS, WE REALIZE THAT TECHNOLOGY HAPPENS.
SO WE ASK FOR YOUR PATIENCE TODAY.
WE HAVE A TECHNOLOGY TEAM HERE TO ADDRESS ANY ISSUES.
IN YOU HAVE SPECIFIC PROBLEMS, E-MAIL US AT PRIVACYCONFTC.GOV AND TRY TO HELP YOU AS QUICKLY AS POSSIBLE.
WE WELCOME QUESTIONS FOR OUR AUDIENCE.
PRIVACYCON IS A PARTICIPATORY EVENT.
WHAT THAT MEANS IS IF YOU HAVE ANY QUESTIONS FOR OUR PANELISTS TODAY, SEND THEM TO US AS PRIVACYCONPRIVACYCON @FTC.GOV.
USE #FTC AND #PRIVACYCON21.
YOU CAN ASK QUESTIONS THROUGH THE LIVE TWEETS AND WE'LL MAKE SURE THAT THEY GET PASSED ON.
I WANT TO THANK ALL OF OUR RESEARCHERS AND PANELISTS.
WE HAVE 19 DIFFERENT PRESENTATIONS.
WHILE ALL THE PEOPLE PRESENTING THE RESEARCH ARE FANTASTIC, WE'RE SO EXCITED FOR THE WORK THEY DONE.
THEY REPRESENT A LOT OF PEOPLE.
THERE'S HUNDREDS OF PEOPLE THAT WORK WITH THE 19 PRESENTERS.
PLEASE GO TO OUR WEBSITE.
YOU'LL SEE ALL THE PAPERS THERE.
YOU CAN READ THEM AND WE'LL PUT UP THE PRESENTATIONS.
WE HOPE YOU ENGAGE WITH THOSE PEOPLE.
MOST OF ALL THE CONTACT INFORMATION IS IN ALL OF THE PAPERS.
WE WANT YOU TO ENGAGE WITH PEOPLE.

IF YOU'RE NOT ABLE TO DO SO, CREATE A DIALOGUE.
SO TODAY'S PROGRAM WOULDN'T BE POSSIBLE WITHOUT A VERY LARGE NUMBER OF PEOPLE.
I JUST WANT TO SAY A COUPLE OF QUICK THANK YOUS.
ALL OF THE PANELISTS TODAY I'D LIKE TO THANK DEVIN WILLIS, DANIELLE ESTRADA, MILES PLANT, LINDA COPP AND KRISTIN YOUNG.
I WANT TO THANK THE MEDIA TEAMS, ALL THE PEOPLE HELPING WITH THE LEAVE STREAM INCLUDING OUR OFFICE OF PUBLIC AFFAIRS.
WE APPRECIATE HELP FROM PEOPLE LIKE JUNE CHANG, BRIANNA JAMES, AND SO MANY OTHER PEOPLE.
TWO SPECIAL THANK YOUS I WANT TO IMAGINE.
THE FIRST IS FOR LEAH HEBRON AND ALEX IGLESIAS.
WITHOUT FURTHER ADIEU, IT'S MY PLEASURE TO INTRODUCE COMMISSIONER REBECCA KELLY SLAUGHTER.
>> EXCUSE ME.
THANK YOU, JAMIE.
THANK YOU TO EVERYBODY WHO WORKS SO HARD TO PUT ON TODAY'S EVENT.
GOOD MORNING!
I'M COMMISSIONER BECCA KELLY SLAUGHTER.
ON BEHALF OF THE FTC AND MY FELLOW COMMISSIONERS, I'M SO PLEASED TO WELCOME YOU TO PRIVACYCON 2021.
THANKS FOR ATTENDING VIRTUALLY THIS YEAR.
WHILE CIRCUMSTANCES HAVE BEEN AND CONTINUE TO BE CHALLENGING FOR ALL OF US, I'M SO GLAD WE HAVE THE TOOLS TO CONVENE SO MANY DISTINGUISHED ADVOCATES, RESEARCHERS, ACADEMICS AND RESEARCHERS FROM AROUND THE COUNTRY AND ACROSS THE GLOBE.
OUR SECOND VIRTUAL CONFERENCE IS A GOOD OCCASION TO NOTE HOW MUCH THE PANDEMIC HAS ACCELERATED OUR RELIANCE ON DIGITAL SERVICES.
PEOPLE TURNING TO ONLINE PLATFORMS AND MARKETPLACES FOR EVERYTHING FROM SOCIALIZING TO SOAP.
THE NECESSITY OF MOVING SO MUCH OF OUR LIVES ONLINE HAS ALSO HIGHLIGHTED CHALLENGES IN THE DIGITAL MARKETPLACE AND THE SERIOUS ISSUES, DATA DRIVEN BUSINESS MODELS POSE TO OUR PRIVACY, AUTONOMY AND SOCIETY AT LARGE.
YOU HAVE A FULL MENU AHEAD OF YOU TODAY.
I WANT TO OPEN THE BUFFET WITH FOOT FOR THOUGHT ON TWO TOPICS.
WE'RE HERE FOR PRIVACYCON.
BUT I'D LIKE TO REJECT EVERYONE TO REJECT PRIVACY AS THE NETWORK FOR THE IMPORTANT ISSUES DISCUSSED AND AMONG THOUGHT LEADERS WITH RESPECT TO OUR DATA-DRIVEN ECONOMY.
TODAY'S AGENDA ADDRESSES ALGORITHMIC BIAS, MISINFORMATION DURING THE PANDEMIC AND SPECIAL CONCERNS RELATED TO KIDS AND TEENS AND PREVENT CONVENTIONAL PRIVACY CONCEPTS.
THE FTC WORKS ON ALL OF THESE FRONTS AND WORKS FRAME WORKS AROUND

DARK PATTERNS.
THESE ISSUES GO BEYOND PRIVACY AS TRADITIONALLY CONCEIVED.
THE BROAD AGENDA REFLECT AS GROWING CONCERN ABOUT THE ISSUES THAT THE COMMISSION AND SOCIETY AT LARGE ARE CONCERNED ABOUT MOVED PASS WHO HAS ACCESS TO YOUR DATA.
THIS UNDERSTANDING IS WHY I PREFER THE TERM "DATA ABUSES" TO THE NARROWER LANGUAGE OF PRIVACY.
WORDS MATTER.
DATA ABUSE REFLECTS THE FACT THAT RAMPANT CORPORATE DATA COLLECTION AND SHARING AND EXPLOITATION HARMS CONSUMERS, WORKERS AND COMPETITION IN WAYS THAT GO BEYOND OUR LIBERTARIAN PRIVACY CONCERNS.
WE MUST EXAMINE A WIDE VARIETY OF DATA INCLUDING QUESTIONS OF RACIAL BIAS, CIVIL RIGHTS AND ECONOMIC EXCLUSION.
CONSIDERING PRACTICES THAT UNDERMINE PERSONAL AUTONOMY AND DIGNITY AND REEVALUATING DANGEROUS BUSINESS MODELS IN THE MARKET.
IN ADDITION TO EXAMINING THESE PRACTICES, WE HAVE TO CONSIDER WHAT TO DO WITH THE PROBLEMS IN THE MARKETS.
THE SECOND CHALLENGE TO ISSUE TODAY IS THE FOLLOWING.
CAN WE MOVE AWAY FROM OUTDATED NOTICE AND CONSENT MODELS TO GOVERN QUESTIONS SURROUNDING PERSON DATA?
INSTEAD TURN OUR FOCUS TO THE UNDERLYING BUSINESS STRUCTURES AND INCENTIVES THAT ARE ANCHORED IN COLLECTION AND APPLICATION OF PERSONAL DATA TO FUEL DATA-DRIVEN BUSINESS MODELS LIKE BEHAVIORAL ADVERTISING.
IT'S THIS UNDERLYING INCENTIVE STRUCTURE THAT HAS CAUSED SO MANY OF THE HARMS AND PRIVACY RISKS WE'RE HERE TO DISCUSS TODAY.
RATHER THAN FOCUSING ON OPT IN VERSUS OPT OUT AND WHETHER PRIVACY POLICIES ARE CLEAR ENOUGH, WE SHOULD DISCUSS DATA MINIMIZIZATION.
ONLY COLLECT THE INFORMATION NECESSARY TO PROVIDE THE CONSUMERS NEEDED.
THAT MINIMIZIZATION COULD BE USED WITH SHARING AND SECURITY REQUIREMENTS TO ENSURE THAT THE INFORMATION COMPANIES CAN PERMISSIBLY COLLECT ISN'T THEN USED TO BUILD TOOLS OR SERVICES THAT IMPERIL PEOPLE'S CIVIL RIGHTS, ECONOMIC OPPORTUNITIES OR PERSONAL AUTONOMY.
CORPORATE SELF-DEALING IS ALSO A PROBLEM.
AS LONG AS KEY DIGITAL MARKETS ARE CONTROLLED BY A FEW DATA HUNGRY PLATFORMS, CONSUMERS AND ENTRANTS ARE AT THEIR MERCY.
I'VE HEARD THE CALL FROM MEMBERS OF THE PUBLIC AT OUR TWO OPEN MEETINGS FOR US TO TAKE ACTIONS AGAINST THESE ABUSES, THIS MOMENT OF RENEWED ENERGY AT THE FTC OFFERS A WINDOW OF TIME TO LOOK AT CHANGES IN THE MARKETS AND ENSURE THAT THE DATA ECONOMY WORKS FOR PEOPLE, NOT JUST THE LARGEST CORPORATE FIRES.
INCHECKED DATA COLLECTION IS NOT JUST A CONSUMER PROTECTION ISSUE.
IT'S A COMPETITION ISSUE.
THE ENORMOUS AMOUNTS OF DATA COLLECTED GIVES THEM A PROFOUND

ADVANTAGE WHEN COMPETING AGAINST NEW ENTRANTS OR SEEKING TO ENTER A NEW PRODUCT MARKET THEMSELVES.
WE ABSOLUTELY MUST LOOK AT THESE ISSUES HOLISTICALLY RATHER THAN VIEWING THEM THROUGH THE CONSUMER PROTECTION.
I BELIEVE THE FTC HAS AN OBLIGATION TO USE ALL TOOLS TO ADDRESS THESE ISSUES.
CHALLENGING THE APPLICATION OF ABUSIVE DATA PRACTICES ISN'T LIKELY TO BRING ABOUT THE SYSTEMIC CHANGE THAT WE NEED TO SEE IN THE MARKETS.
THE FTC HAS BENEFITTED FROM WORKSHOPS AND CONFERENCES LIKE THIS ONE.
I HOPE PARTICIPANTS AND OBSERVERS OF TODAY'S CONFERENCE HELP US CHART A PATH FORWARD TO BUILD A MORE FAIR AND JUST FUTURE TOGETHER.
THANKS AGAIN TO EVERYONE FROM THE FTC THAT MADE TODAY'S EVENT POSSIBLE.
TO OUR ATTENDEES, I GRATEFUL FOR YOUR WORK AND HOPE TO HEAR FROM YOU AT THE COMMISSION.
IT'S NOW MY HONOR AND PLEASURE TO LOOK AT THE CHIEF TECHNOLOGIST FOR OPENING REMARKS.
>> THANK YOU COMMISSIONER SLAUGHTER.
TO EVERYONE WHO PUT ON TODAY'S EVENT, ESPECIALLY JAMIE HINE AND OUR WONDERFUL PRESENTERS, THANK YOU NOR TODAY AND ALL THE WORK THAT LED TO TODAY.
I'M ERIE MEYER AND I'M AN ADVISER TO FTC CHAIN LEENA KHAN.
I WAS LIVING IN CENTRAL OHIO DURING THE HEIGHT OF THE FINANCIAL CRISIS.
I WATCHED FAMILIES I HAD KNOWN LOSE THEIR HOMES BECAUSE OF THE GOVERNMENT'S FAILURE TO REIGN IN DEVASTATING INDUSTRY ABUSES.
IT BROKE MY BRAIN.
I HAD SEEN MYSELF AS A TECH PERSON BEFORE.
BUT NOW I JUST DIDN'T WANT TO DESIGN MULTIVARIANT TESTS TO IMPROVE AD CONVERSION RATES.
I WANTED TO MAKE SURE THE BIG GUYS HAD TO FOLLOW THE LAW AND TO ENSURE MY NEIGHBORS WERE TREATED LIKE HUMAN BEINGS.
BEFORE WE KICK OFFER TODAY'S EVENT, I WANT TO SHARE A FEW PLACES WHERE THE MARKET SHOULD EXPECT CHANGES AND HOW THE FTC WILL APPROACH ITS WORK WHEN IT COMES TO PROTECTING THE PUBLIC FROM THE MISUSE AND ABUSE OF DATA.
THE APPROACH IS NOT THROUGH A NARROW LENS OF CONSUMER PROTECTION.
DATA ABUSES DON'T HAPPEN IN A VACUUM.
THEY'RE FED BY INCENTIVES.
AMONG THEM BEATING OUT COMPETITORS.
SO WITH THAT BROADER VIEW, YOU CAN EXPECT KEY CHANGES IN OUR WORK.
WE'RE GOING TO MAKE SURE THAT DATA ABUSERS FACE CONSEQUENCES FOR THE WRONG DOING AND PROVIDE REAL HELP FOR AFFECTED INDIVIDUALS.
WHEN A FIRM BREAKS THE LAW OR WORSE, BREAKS THE LAW OVER AND OVER AND OVER, REGULATORS LIKE THE FEDERAL TRADE COMMISSION NEED TO DESIGN AND IMPOSE REMEDIES THAT FIX THINGS.

FIXING THINGS DOESN'T MEAN MAKING A DISCLOSURE LONGER OR A ONE-TIME FIND BIGGER.
IT MEANS MAKING SURE THAT THE FIRM CANNOT AND WILL NOT BENEFIT FROM ILL-GOTTEN DATA INCLUDING AGAINST THEIR COMPETITORS.
IT MEANS MAKING SURE THAT THE REST OF THE INDUSTRY IS DETERRED FROM ENGAGING IN SIMILAR WRONGDOING.
MIGHT MEAN THAT WE NEED TO LOOK AT RESTRUCTURING BUSINESS INCENTIVES OR CORPORATE STRUCTURE.
IT MEANS MAKING SURE THAT THE PEOPLE THAT ARE TARGETED OR HURT ARE ABLE TO UNDERSTAND WHAT HAPPENED TO THEM AND TO GET HELP, ACTUAL HELP.
WHAT DOES THIS LOOK LIKE IN PRACTICE?
LOOKS LIKE COMPANIES THAT BREAK THE LAW HAVING TO NOT JUST SCOURGE DATA AND MONEY BUT ALGORITHMS THAT WERE JUICED BY ILL-GOTTEN DATA.
COMPANIES THAT SACRIFICED SECURITY AND SERVICE OF SPEED BEING SUBJECT TO BANS JUST LIKE ABUSE OF DEBT COLLECTORS.
PRESIDENT PEOPLE GETTING THE DIGNITY OF SPECIFIC AND CLEAR BUT MOST IMPORTANTLY USABLE INFORMATION ABOUT WHAT HAPPENED TO THEM AND WHERE THEY CAN CONNECT WITH STRAIGHT ANSWERS ABOUT WHAT IS NEXT.
TURNS OUT THAT PAPERWORK CAN'T FIX THE FUNDAMENTAL PROBLEM.
DATA ABUSE IS NOT JUST AN ISSUE OF PRIVACY.
IT'S A MATTER OF CIVIL RIGHTS AND NATIONAL SECURITY.
PEOPLE FROM COMMUNITIES WHOSE RIGHTS AND SAFETY ARE CONSTANTLY THREATENED CAN TELL YOU, THIS ISN'T JUST ABOUT SOMEONE KNOWING WHAT YOU'VE LOOKED UP ONLINE.
THE U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT CHARGED FACEBOOK WITH VIOLATING THE FAIR HOUSING ACT.
THE DEPARTMENT OF JUSTICE CHARGED A ZOOM EXECUTIVE ALLEGING THAT HIS ACTIONS LED TO PEOPLE USE ZOOM'S DATA TO TRACK DOWN AND INTIMIDATE FAMILY MEMBERS OF PEOPLE WHO USE THE PLATFORM TO DISCUSS THE TIANANMEN SQUARE MASSACRE.
THERE'S BEEN A 2,920% INCREASE IN REPORTS OF IDENTITY THEFT VIA GOVERNMENT BENEFITS THIS YEAR.
SO WHAT THIS MEANS, FOR EXAMPLE, IS WHEN A BAD ACTOR APPLIES FOR SOMETHING LIKE UNEMPLOYMENT BENEFITS USING PERSONAL INFORMATION GLEANED FROM A DATA BREACH FROM ONE OF THESE FIRMS.
I SINCERELY HOPE NONE OF YOU HEARD PEOPLE YOU LOVE CRY THIS YEAR BECAUSE THEY LOST THEIR JOBS IN THE PANDEMIC AND STRUGGLED TO ACCESS BENEFITS.
BUT I DID.
I WANT TO RE-AFFIRM THAT THE RECKLESSNESS OF FIRMS THAT THINK THEY THEY CAN GET AWAY WITH NOT KEEPING THEIR PROMISES ABOUT PROTECTING DATA AND THINK IT'S A SCANDAL RATHER THAN A SYSTEM IS RESULTING IN FAMILIES IS, REAL FAMILIES YOU KNOW NOT HAVING ENOUGH MONEY TO BUY FOOD.
A PANDEMIC HAS SHARPENED THE VIEW OF WHAT HAPPENED TO OUR COUNTRY'S

RESILIENCE BECAUSE OF THESE DATA DISASTERS.
WE'RE MOVING AWAY FROM A LEGALISTIC APPROACH.
THIS MEANS WE'LL BE APPROACHING INVESTIGATIONS WITH A DISCIPLINARY LENS INCLUDING PRIVACY ENGINEERS AND DESIGNERS, FINANCIAL ANALYSTS AND PRODUCT MANAGERS AND YES, TECHNOLOGISTS.
THIS WON'T HAPPEN OVERNIGHT.
WE'VE HER BEGUN TO ASSEMBLE TO MAKE SHIFTS, SHARPENING OUR ANALYTICAL APPROACH.
I'M PLEASED THAT STEPHANIE NGUYEN HAS JOINED OUR TEAM AND WE'RE WORKING TO DRIVE MANY OF THESE EFFORTS.
ONE OF THE PIONEERS OF PRIVACY ENGINEERING, LEAH KISSNER ONCE TOLD ME TO TELL THE WAY A PRIVACY FIX WOULD BE MEANINGFUL WAS THAT IF A LAWYER COULD DO IT ALONE, IT WASN'T ACTUALLY GOING TO CHANGE ANYTHING.
LEAH IS RIGHT.
IF A COMPANY CAN COME IN TO COMPLIANCE BY PAPERING OVER QUESTIONABLE CONDUCT, IT'S NOT CHANGING THE FACTS ON THE GROUND.
SO TO ALL THE OTHER PEOPLE THAT MIGHT BE TIRED OF WORKING ON DESIGNING MULTIVARIANT TESTS TO IMPROVE AD CONVERSION RATES, HELP US CHANGE THE FACTS ON THE GROUND.
WE'RE HIRING.
IN CLOSING, I WANT TO JOIN MY COLLEAGUES IN THANKING THE INCREDIBLE TEAM THAT PUT ON THIS EVENT AND TO WELCOME YOU ALL HERE TODAY TO OUR DISCUSSION AS THE FTC CHARTS A NEW APPROACH TO POLICING DATA ABUSES ON OUR ECONOMY.
NOW TO PANEL 1.
>> GOOD MORNING.
I'M DEVIN WILLIS, AN ATTORNEY FROM PRIVACY AND IDENTITY PROTECTION IN THE FTC.
I'D LIKE TO WELCOME YOU TO THE FIRST PANEL OF PRIVACYCON OF 2021 TILED "ALGORITHMS."
LAST YEAR WE HAD AN INTERESTING PANEL FOR AI ALGORITHMS.
WE HAVE THREE PANELISTS WITH VERY INTERESTING TAKES ON ALGORITHMS.
FIRST, WE'LL HEAR FROM BASILEAL IMANA FROM THE UNIVERSITY OF SOUTH CAROLINA.
NEXT, HONGYAN CHANG FROM THE NATIONAL UNIVERSITY OF SINGAPORE WILL PRESENT HER PAPER ON THE PRIVACY RISKS OF ALGORITHMIC FAIRNESS.
FINALLY, MARTIN STROBEL FROM THE NATIONAL UNIVERSITY OF SINGAPORE WHO WILL CONCLUDE THE PRESENTATION PORTION OF OUR PANEL DISCUSSING HIS PAPER ENTITLED ON THE PRIVACY RISKS OF MODEL EXPLANATIONS WHICH STUDY TOOLS USED TO PROVIDE ALGORITHMIC EXPLAINABILITY.
MORE DETAILS BIOS OF OUR PANELISTS AND LINKS ARE AVAILABLE ON THE PRIVACYCON 2021 WEBSITE AT FTC.GOV.
AFTER WE CONCLUDE THE PRESENTATION PORTION, WE HAVE A QUESTION AND ANSWER PERIOD TO TAKE QUESTIONS AS TIME PERMITS.

IF YOU HAVE QUESTIONS, YOU CAN E-MAIL US OR SENT VIA TWITTER.
I'D LIKE TO TURN TO BASILEAL TO STARTED US OFF.
>> ALL RIGHT.
THANK YOU, DEVIN, FOR THE INTRODUCE.
I'M BASI AND I'M A STUDENT AT THE UNIVERSITY OF SOUTHERN CALIFORNIA.
I'LL TAKE OUR AUDITING FOR DISCRIMINATION.
THIS IS JOINT WORK DONE IN COLLABORATION WITH MY PH.D.
ADVISERS.
TARGET ADVERTISEMENT HAS BECOME POPULAR IN RECENT YEARS AND ONE OF THE WAYS THAT PEOPLE ACCESS OPPORTUNITIES LIKE EMPLOYMENT OR EDUCATION CREDIT AND HOUSING.
THEREFORE EXTERNALLY AUDITING THE ROLE THAT THESE ALGORITHMS PLAY IN SHAPING SOCIETY IS IMPORTANT TO ENSURE THAT THE ADS ARE BEING DELIVERED IN A FAIR WAY AND ALSO THAT THEY'RE BEING COMPLIANT WITH APPLICABLE LAWS LIKE IN REGULATED DOMAINS SUCH AS EMPLOYMENT.
NEXT SLIDE.
SO I'LL START OFF WITH AN EXAMPLE.
LET'S SAY I'D LIKE TO HIRE A SOFTWARE ENGINEER.
I CREATE A DIGITAL AD.
I WANT TO TARGET SO I CREATE A GENDER BALANCE.
SO WITH 50 FEMALES, 50 MALES.
I RUN THIS AD ON FACEBOOK.
THEN THE OUTCOME I GET IS THAT MORE FRACTIONAL FEMALES SEE THE ADS T QUESTION IS WHY IS THERE GENDER SKEWS THE OUTCOME EVEN THOUGH I TARGETED A GENDER BALANCED AUDIENCE?
ONE REASON MIGHT BE BECAUSE THERE'S MORE FEMALES AT THIS TIME THE AD WAS BEING RUN.
BUT THERE MIGHT BE OTHER FACTORS.
WE LOOKED AT THIS QUESTION AND CONTROL FOR COMPOUNDING FACTORS AND SHOWED THAT THE ROLE THAT FACEBOOK'S AD ALGORITHMS PLAY IN DECIDING WHO SEES AN AD IS THE CAUSE FOR SKEWED OUTCOMES.
WHAT THIS DID NOT LOOK AT IS THE ROLE THAT QUALIFICATIONS MIGHT PLAY IN THE OUTCOME.
SO WE GO BACK TO THIS EXAMPLE AND LOOK AT WHAT FRACTIONAL MALES AND FEMALES IN THE AUDIENCE ARE QUALIFIED FOR THE JOB BEING ADVERTISED AND USE THAT TO INTERPRET THE OUTCOMES.
WE CAN SEE THAT IT CAN BE EXPLAINED BY THE DIFFERENCES IN QUALIFICATION BETWEEN MALES AND FEMALES.
LOOKING AT QUALIFICATION IS IMPORTANT FROM THE LEGAL PERSPECTIVE BECAUSE COMPANIES ARE ABLE TO USE IT AS A LEGAL JUSTIFICATION AGAINST CLAIMS OF DISCRIMINATION.
SO WE WANT TO RULE OUT QUALIFICATIONS LIKE COMPANIES USING THAT TO RULE OUT AUDIT FINDINGS THAT SHOW DISCRIMINATION.
SO BASED ON THIS, OUR MAIN CONTRIBUTE TO GIVE A NEW METHOD FOR AUDITING

DISCRIMINATION AND THE JOB AD.
WE TAKE THIS METHOD AND WE STUDY AD DELIVERY ON TWO PROMINENT AD PLATFORMS, LINKEDIN AND FACEBOOK.
WE FIND RESULTS THAT SHOW DISCRIMINATORY BY GENDER IN THE CASE OF FACEBOOK WHEREAS WE FIND NO SUCH EVIDENCE IN LINKEDINS CASE.
NEXT SLIDE.
SO HOW WE ACCOUNT FOR QUALIFICATION AS THE MAIN PART OF OUR CONTRIBUTION.
I'LL FOCUS ON THAT.
THERE'S MORE IN THE PAPER.
SO THE MAIN CHALLENGE WITH ACCOUNTING FOR QUALIFICATION IS THAT EXTERNAL AUDITORS, WE DON'T HAVE ACCESS TO USER PROFILE DATA THAT WOULD LET US DIRECTLY CONTROL FOR QUALIFICATION AND THE AUDIENCE TARGETED WHILE WE RUN ADS.
WE RELY ON AN INDIRECT APPROACH.
SO WE FIND A PAIR OF JOB POSITIONS WITH TWO CONDITIONS.
FIRST, THEY MUST HAVE SIMILAR QUALIFICATION REQUIREMENTS.
SECOND THERE MUST BE A GENDER SKEW IN THE REAL WORLD.
SO TO GIVE AN EXAMPLE, IF WE TAKE DELIVERY DELIVER JOBS LIKE DOMINOES VERSUS INSTACART, ONE IS PIZZA DELIVERY, ONE IS GROCERY DELIVERY, 98% OF DOMINOES DRIVERS ARE MALE AND MAJORITY OF INSTACART ARE FEMALE EVEN THOUGH BOTH JOBS HAVE SIMILAR QUALIFICATION REQUIREMENTS.
SO WE TAKE THE JOBS AND WE RUN ADS FOR THEM AT THE SAME TIME.
WE LOOK AT THE OUTCOME.
SO WE LOOK AT WHETHER THERE'S A RELATIVE DIFFERENCE IN HOW THESE ADS ARE DELIVERED BY GENDER.
BECAUSE WE CONTROL QUALIFICATION AND THOSE CONFOUNDING FACTORS, IF WE SEE A DIFFERENCE, WE HYPOTHESIZE IT'S DUE TO THE PLATFORMS AD DELIVERY ALGORITHMS.
SO IN THIS CASE, WE WOULD EXPECT THE INSTACART AD TO BE SHOWN TO MORE FEMALES IF THE PLATFORM IS PERPETRATING THE EXISTING SKEW.
NEXT SLIDE.
SO WE TAKE THIS METHODOLOGY AND WE REGISTER AS ADVERTISERS ON LINKEDIN AND FACEBOOK AND WE RUN ADS.
TO SHOW ONE OF OUR RESULTS FOR THE INSTACART AND DOMINO'S EXAMPLE.
SO IF YOU LOOK AT THE SLIDE, THE X AXIS ON THE PLOT IS THE FRACTIONAL FEMALES THE AD WAS SHOWN TO AND THE Y AXIS IS THE TWO PLATFORMS THAT WE STUDIED, FACEBOOK AND LINKEDIN.
ON THE RIGHT-HAND SIDE WE HAVE THE RESULT OF THE TEST THAT WE APPLIED TO TESTS WHETHER THE SKEW IS INDEED SIGNIFICANT.
SO IF WE LOOK AT THE TOP ROW, WE CAN SEE THE INSTACART AD IS SHOWN TO HIRE FEMALES.
ON THE OTHER HAND, ON THE BOTTOM ROW, WE CAN SEE THERE'S NO DIFFERENCE BETWEEN THE INSTACART AND THE DOMINO'S AD.

OVERALL, THIS RESULT SHOWS THE SKEW ON FACEBOOK BECAUSE WE CONTROL FOR QUALIFICATION IS NOT JUST EXCUSED BY DISCRIMINATING IN THE LEGAL SENSE AND THE ROLE THAT FACEBOOK'S AD ALGORITHMS ARE PLAYING TO THIS DISCRIMINATORY OUTCOME.
THIS RESULT IS JUST ONE INSTANCE OF OUR EXPERIMENT.
WE REPEAT THIS ON MULTIPLE AUDIENCES AND DIFFERENT JOB CATEGORIES AND WE FIND THE RESULTS.
NEXT SLIDE.
NEXT WE LOOKED AT WHETHER THIS SKEW ON FACEBOOK'S CASE IS MERELY DUE TO FACEBOOK OPTIMIZING FOR CLICKS OR ENGAGEMENT, WHICH IS SOMETHING AN ADVERTISER MIGHT BE INTERESTED IN.
SO WHAT WE DO IS WE LOOKED AT THE ADVERTISING OBJECTIVES THAT ADVERTISERS CAN CHOOSE WHEN CREATING AN AD.
WE COMPARED TO OBJECTIVES.
THE FIRST IS REACH OBJECTIVE, WHICH THE AIM IS TO SHOW ADS TO AS MANY PEOPLE AS POSSIBLE IN THE TARGETED AUDIENCE AND THE OTHER OBJECTIVE IS CONVERSION, WHICH SHOWS THE AD TO PEOPLE WHO ARE MORE LIKELY TO APPLY FOR THE JOB BEING ADVERTISED.
SO WHILE WE WERE INTERESTED IN TO RUN THE ADS WITH BOTH OBJECTIVES TO COMPARE AND SEE WHETHER ADVERTISERS CAN REACH A MORE WIDER AUDIENCE BY USING A REACH OBJECTIVE.
IF YOU LOOK AT THE PLOT ON THIS SLIDE.
IT'S A SIMILAR GRAPH BUT IN THIS CASE THE Y AXIS SHOWS THE REACH IN CONVERGENCE CASE.
BOTH ARE RUN ON FACEBOOK AD PLATFORMPLATFORMS.
IN BOTH CASES THE ADS ARE SKEWED WHICH SHOWS THAT FACEBOOK'S ALGORITHMS AD DELIVERY EVEN IF THE ADVERTISER USES THE REACH OBJECTIVE TO TRY TO REACH A MORE WIDER AUDIENCE, AGAIN, FOR THIS EXPERIMENT.
IN LIGHT OF THIS RESULT TO DISCUSS POLICY IMPLICATIONS OF OUR WORK, WHAT OUR TECHNICAL EVIDENCE HAS SHOWN IS THAT THE ROLE THAT AD DELIVERY ALGORITHMS PLAY IN AD DELIVERY IS IMPORTANT IN THAT REGULATION NEEDS TO TAKE THIS INTO CONSIDERATION.
AND THE QUESTIONS THAT WE WOULD LIKE POSE AN INTERESTING THOUGHT.
THIS TECHNICAL EVIDENCE SUFFICIENT TO ENACT NEW POLICIES THAT WILL MANDATE AD PLATFORMS TO CHANGE HOW THEIR AD DELIVERY ALGORITHMS WORK N THE PAST LEGAL CHALLENGES AND CIVIL RIGHTS AUDITS HAVE PUSHED AD PLATFORMS TO CHANGE HOW THEIR AD TARGETS WORKS.
SO WE HOPE TO SEE SIMILAR ACTION IN THE CONTEXT OF AD DELIVERY.
THE OTHER QUESTION IS, ARE THERE OTHER ADDITIONAL TECHNICAL INSIGHTS OR AUDITS THAT WOULD BE USEFUL TO HELP FORMULATE FUTURE POLICIES FOR GOVERNMENT --
GOVERNING AD PLATFORMS.
IN CONCLUSION IN OUR WORK, WE HAVE SHOWN THAT AD PLATFORMS SHOULD CHANGE HOW THE DELIVERY ALGORITHMS WORK FOR OPPORTUNITY ADS LIKE

EMPLOYMENT.
WE HOPE THAT REGULARS CAN USE OUR METHODOLOGY AND FINDINGS TO INFORM FUTURE POLICIES.
WITH THAT I'LL CONCLUDE MY TALK.
OUR DATA CAN BE FIND AT THE LINK ON THE SLIDE.
THANK YOU.
>> THANK YOU, BASI.
LET'S MOVE NEXT TO HONGYAN.
>> HELLO.
OKAY.
THE NEXT DATA FOR OUR PREVIOUS INTRODUCTION.
I'M HONGYAN CHANG FROM NATIONAL UNIVERSITY OF SINGAPORE.
VERY HAPPY TO BE HERE TO GIVE YOU ANOVER VIEW OF OUR WORK TITLED PRIVACY RISK OF ALGORITHM FAIRNESS.
FAIRNESS.
ALGORITHMIC FAIRNESS AND PRIVACY ARE ESSENTIAL PARTS OF LEARNING.
THIS WORK FOCUSES ON SOLVING ONE PROBLEM SUCH AS DESIGNING PRIVACY, PRESERVING THE ALGORITHMS.
TIME OR IN REAL LIFE, FAIRNESS AND PRIVACY DO NOT INVEST IN ISOLATION.
SO A DEEPER UNDERSTANDING OF RELATIONSHIPS BETWEEN FAIRNESS AND PRIVACY IS NECESSARY.
SO IN OUR PAPER, WE TRY TO FIND THE COST OF PRIVACY AND ACHIEVING FAIRNESS.
ONE COUNTER INTUITIVE FACT IS THAT MODELS ARE NOT NEUTRAL.
MOST IMPRESSIVE EXAMPLE IS THAT RACIAL BIAS IS A POPULAR COMMERCIAL ALGORITHM USED BY JUDGES AND CRIME.
IT HAS SHOWN THE ALGORITHM IS BIASSED IN FAVOR OF WHITE DEFENDANTS AND AGAINST BLACK DEFENDANTS.
IN THE NEXT SLIDES, LET'S SAY WHITE MODELS ARE BIASSED.
BIASSED CAN BE INTRODUCED IN TO ALGORITHMS.
THE TRENDING DATA IS COLLECT WHILE BIASSED.
THIS HUMAN BIAS IS USED TO THE DATA SET AND ULTIMATELY TO THE PREDICTION OF THE MODEL.
THE LEARNING ALGORITHM ITSELF MAY INTRODUCE BIAS.
THE MODEL TENDS TO FIT THE MAJORITY GROUP BETTER AS THE PRIMARY UNDERSTANDING OF ALGORITHM IS TO LEARN THE MINIMIZING LOSS, WHICH ITSELF FAVORS THE MAJORITY.
THE NEXT SLIDES, LET ME GIVE YOU AN OVERVIEW ABOUT ALGORITHMIC FAIRNESS.
MOST FAIRNESS DEFINITIONS HAVE BEEN PROPOSED TO REGULATE THE PREDICTION BEHAVIOR OF THE LEARNED MODEL.
[INAUDIBLE]
-- IDENTIFIED BASED ON ATTRIBUTES LIKE RACE, GENDER.
MOST SPECIFICALLY WE SEE A MODEL IS FAIR WHEN THE TRUE RATE AND TNR ARE SIMILAR.

ACCORDINGLY THE FAIRNESS OF A MODEL SHOWS THE GAP IN THE RATES BETWEEN GROUPS AS FAIRNESS GAP.
FROM NOW ON, LET'S FOCUS ON TEAM ATTRIBUTES.
WE FOCUS ON THE PERFORMANCE DIFFERENCES OF TWO PROTECTED GROUPS.
BASED ON THIS DEFINITION, MOST OF EXISTING ALGORITHMS TRY TO FORM A MODEL THAT MINIMIZE THE AVERAGE LOSS WHILE SATISFYING THE COST OF TRAIN DAMAGE THAT.
LET ME GIVE YOU AN EXAMPLE TO SHOW YOU HOW THEY WORK.
SUPPOSE A UNIVERSITY WANTS TO BUILD A LINEAR MODEL BASED ON THE SAT SCORE AND THE JPA OF APPLICANTS IN HIGH SCHOOL.
THERE'S TWO POPULATIONS.
THE UNIVERSITY SHOWS THE HISTORICAL DATA WHICH HAS DIFFERENT PEOPLE AS SHOWN IN THE FIGURE HERE.
POSITIVE AND NEGATIVE RESPECTIVELY.
NEXT, LET'S LOOK AT THE STANDARD MODEL.
WE CAN LEARN THIS DATA SET.
IN THIS SETTING, THE UNIVERSITY WHERE WE HAVE A MODEL REPRESENTED BY THIS RED LINE HERE T MODEL PERFORMS BETTER ON THE BLUE PEOPLE.
AS A RESULT OF MINIMIZING THE AVERAGE LOSS.
IN THIS CASE, THE YELLOW GROUP IS THE UNDERPRIVILEGED GROUP.
NEXT, TO ACHIEVE FAIRNESS, WE MAY WANT TO USE THE MODEL REPRESENTED BY THIS GREEN LINE.
HOWEVER, USING THIS GREEN LINE CAN CAUSE PRIVACY ISSUE.
LET ME EXPLAIN WHY.
SO TO ACHIEVE FAIRNESS, A FAIR ALGORITHM PLACE THIS GREEN LINE RIGHT UNDER SOME YELLOW POINTS WITH POSITIVE LABELS.
IN OTHER WORDS, AN INCREASE IS THE INFLUENCE FROM THE UNDERPRIVILEGED GROUP.
ORIGINALLY THE STANDARD MODEL, THE RED LINE REVEALS LITTLE INFORMATION ABOUT YELLOW APPLICANT.
NOW THAT THE GREEN LINE IS RIGHT UNDER SOME YELLOW POINTS, SO INTUITIVELY MORE INFORMATION ABOUT THE YELLOW POINTS.
FAIRNESS CAN CAUSE PRIVACY ISSUE ESPECIALLY FOR THE UNDERPRIVILEGED GROUP I THE NEXT SLIDES, LET ME CLARIFY WHAT I MEAN BY PRIVACY.
WE USED TO WIDELY ACCEPT THE PRIVACY DEFINITION.
ROUGHLY SPEAKING, WE'RE SEEING A LEARNING ALGORITHM AS PRIVACY PRESERVING AS WHETHER A INDIVIDUAL WAS PART OF THE ASSETS OR NOT HAS LATER INFLUENCE ON THE LEARNED MODEL.
SO TO QUANTIFY THE PRIVACY, MAKE USE OF THE MEMBERSHIP, THE GOAL IS TO INFER WHETHER A DATA POINT WAS PART OF THE ASSETS OR NOT.
SO A HIGHER ATTACK ACCURACY REFLECTS A HIGHER RATE.
SO WE USE ATTACK ACCURACY.
[INAUDIBLE]
I HAVE THE DETAILS ABOUT THE ATTACK ALGORITHM.

IF YOU'RE INTERESTED, CHECK OUR PAPER FOR MORE DETAILS.
THE LINK OF THE PAPER IS AT THE END OF THE SLIDES.
GREAT.
IN THE NEXT SLIDES, LET ME SHOW YOU THE RESULTS OF THE SYNTHETIC DATA FIRST.
WE HAVE TWO PROTECTED GROUPS.
YELLOW GROUP AND BLUE GROUP.
THE LABELS POSITIVE AND NEGATIVE.
SO WE HAVE FOUR SUBGROUPS.
THE FEATURES FOR THE SUBGROUPSSUBGROUPS --
[INAUDIBLE]
THE BLUE GROUP IS THE MAJORITY GROUP.
HERE I SHOW YOU THE RESULTS OF THE DATA FOR TWO PROTECTED GROUPS WITH POSITIVE LABEL.
THE ACCESS IS A PRIVACY RISK AND THE Y AXIS IS TRAINING.
WE CAN SEE THAT STANDARD MODEL PERFORMANCE MATCH BETTER ON THE BLUE GROUP COMPARED WITH THE YELLOW GROUP.
IF WE USE TO CHOOSE THEIR MODEL, THE YELLOW GROUP HAVE A BETTER ACCURACY.
HOWEVER, THE PRIVACY RISK FOR THE YELLOW GROUP IS ALSO INCREASED AT THE SAME TIME.
FAIR MODEL INCLUDE ACCURACY, BUT LEAKS MORE INFORMATION ABOUT THIS UNDERREPRESENTED GROUP.
UNPRIVILEGED GROUP.
THE NEXT SLIDES, LET'S SEE THE TRADE-OFF BETWEEN FAIRNESS AND PRIVACY.
VARIES WITH DISTRIBUTION OF THE DATA.
EACH SHOWS THE RESULT FOR ONE SETTING.
THE X AXIS SHOWS THE FAIRNESS GAP OF THE STANDARD MODEL WITH RESPECT TO EQUALIZED AND REFLECTING THE FAIRNESS OF THE MODEL T WHETHER AXIS IS A PRIVACY COST FOR THE UNDERPRIVILEGED GROUP.
THE PRIVACY COST IS MIRED AS DIFFERENCES IN THE PRIVACY RISK BETWEEN STANDARD MODEL AND FAIR MODELS.
WE CAN SEE A CLEAR TREND THAT WHEN THERE'S MORE NEEDS FOR FAIRNESS, PRIVACY COSTS ARE HIGHER.
WE ALSO COME BACK TO EXPERIMENTS.
THE NEXT SLIDES, I SHOW YOU THE RESULTS OF THE COMPAS DATA SET.
WE HAVE FOUR GROUPS IDENTIFIED BY RISK AND THE TRUE LABEL.
WE CAN SEE THE PRIVACY RISKS ARE INCREASED FOR THE SUBGROUPS.
THE INCREASE IS DIFFERENT FOR SUBGROUPS.
SO LET ME CONCLUDE MY TALK IN THE NEXT SLIDES.
THE TAKE-AWAYS FROM OUR EMPIRICAL RESULT IS GROUP FAIRNESS BASED ON EQUALIZING ARROW COMES AT A COST OF PRIVACY.
THIS PRIVACY COST IS NOT DISTRIBUTED EVENLY ACROSS GROUPS.
AS A RESULT, IN PRACTICE, IF WE TRY TO PROTECT THE UNDERPRIVILEGED GROUP

USING ALGORITHMS, WE MUST BE VERY CAREFUL BECAUSE IT MAY INCREASE THE PRIVACY RISK.
THANK YOU AND I'M LOOKING FORWARD TO OUR DISCUSSION.
>> THANKS, HONGYAN.
WE CAN MOVE TO YOU, MARTIN.
>> THANKS.
A WONDERFUL MORNING TO EVERYONE.
MY NAME IS MARTIN STROBEL.
I'M A FOURTH YEAR PH.D.
CANDIDATE HERE AT THE UNIVERSITY OF SINGAPORE.
I WANT TO TALK ABOUT PRIVACY RISKS THAT CAN OCCUR WHEN YOU TRY TO EXPLAIN MACHINERY MODELS.
NEXT SLIDE.
SO GIVEN THAT THIS CONFERENCE IS CALLED PRIVACYCON, I ASSUME MOST OF YOU ARE MORE FAMILIAR WITH PRIVACY RISKS THAN THEY ARE WITH EXPLAINING MACHINERY MODELS.
I'M GOING TO SPEND TIME MOTIVATING EVERYONE TO EXPLAIN THE MACHINE LEARNING MODELS.
THERE'S THREE ARGUMENTS FOR WHY YOU WANT TO EXPLAIN A MODEL.
THE FIRST IS IT GIVES AGENCY TO INDIVIDUALS.
SO ASSUME YOU HAVE CUSTOMER, A USER.
THE DECISION WAS MADE BY A MACHINE.
NOW THE PERSON IS UNHAPPY WITH THIS DECISION.
SHOULD HAPPEN FROM TIME TO TIME.
IT'S IMPOSSIBLE FOR A PERSON TO ARGUE AGAINST THIS POSITION IF YOU UNDERSTAND IT.
IF YOU HEARD A HORROR STORY OF DECISION MIGHT CHANGE IF YOU WRITE MAIN STREET INSTEAD OF MAIN ST AND YOU WANT TO UNDERSTAND HOW THE DECISION WAS MADE SO YOU CAN CHANGE IT.
ON A LARGER LEVEL, AGENCIES LIKE THE FTC WANT TO GO IN AND AUDIT A MODEL.
IF YOU JUST LOOK AT THE BIG MODEL, IT'S REALLY HARD TO AUDIT IT.
SO YOU WANT TO BE ABLE TO EXPLAIN THE MODEL.
SO YOU CAN AUDIT IT.
FOR EXAMPLE, IF YOU WANT TO LOOK AT WHETHER OR NOT THE MODEL IS FAIR.
THE FINAL ARGUMENT YOU MIGHT HAVE HEARD IS THE RIGHT TO FAIRNESS.
IT'S MORE LIKE A PHILOSOPHICAL ARGUMENT THAT SAYS IT'S INHERENTLY INHUMANE TO BE SUBJECTED TO A BLACK BOOK DECISION.
SO EVEN IF YOU DON'T WANT TO CHANGE IT OR YOU CANNOT CHANGE IT, IT'S STILL BETTER TO KNOW HOW IT WAS MADE.
THESE THREE ARE LIKE KEY ARGUMENTS FOR WHY YOU WANT TO EXPLAIN.
THE NEXT SLIDE, LET'S LOOK AT HOW NOT TO ACHIEVE.
SO SOME PEOPLE HAVE PROPOSED THAT YOU CAN JUST RELEASE THE ENTIRE MACHINE-RUNNING MODEL.
JUST DUMP IT OUT THERE.

THE FIRST PROBLEM FROM A PRIVACY PERSPECTIVE IS THAT WE ALREADY KNOW THATTHERE'S A MODEL.
THE ADVERSTY THAT CAN LEARN A LOT ABOUT THE DATA.
THERE'S A LOT OF INFORMATION THAT CAN BE OBTAINED AS SOON AS THEY HAVE ACCESS TO YOUR MODEL.
YOU DON'T WANT TO DUMP THE MODEL OUT THERE.
WHOEVER CREATED THE MODEL HAS AN INTEREST IN IT NOT BEING RELEASED.
SECOND, IT'S ACTUALLY NOT GREAT.
MODERN MACHINE MODELS HAVE MILLIONS OF PRIVACIES.
GIVING UP THAT TO SOMETHING LIKE A USER DOESN'T EXPLAIN ANYTHING.
THEY HAVE A LOT OF DATA ON THEIR COMPUTER SO YOU DON'T REALLY ACHIEVE EXPANDABILITY.
SO ON THE NEXT SLIDE, YOU SEE HOW YOU ACHIEVE EXPANDABILITY.
A TYPICAL FRAME WORK ACADEMIA HAS COME UP WITH, INSTEAD OF TRYING TO EXPLAIN AN ENTIRE MODEL, YOU ONLY WANT TO EXPLAIN ONE PROBLEM AT A TIME.
AT THE BOTTOM YOU HAVE THIS TYPICAL SIMPLIFIED MACHINING PIPELINE.
YOU HAVE DATA.
YOU TRAIN A MODEL.
THE MODEL MAKES PREDICTIONS FOR THE USER.
ON TOP OF THIS, YOU PUT AN EXPLAINING FRAME WORK.
THAT INTERACTS WITH THE MODEL AND POTENTIALLY INTERACTS WITH THE DATA AND IT PROVIDES AN EXPLANATION TO THE USER.
THIS OPENS UP POTENTIAL LEAKAGE ON THE NEXT SLIDE.
POTENTIALLY THREE WAYS HOW THIS MODEL MIGHT LEAK SENSITIVE INFORMATION.
ONE IS ALREADY KIND OF COVERED BY HONGYAN.
THE MODEL CAN LEAK MODEL INFORMATION.
HOWEVER, WITH THE EXPLANATION, WE HAVE TWO MORE PIPELINES KIND OF.
THE ONE IS THE EXPLANATION INTERACTS WITH THE DATA CORRECTLY AND MIGHT LEAK INFORMATION AND THE EXPLANATION ALSO INTERACTS WITH THE MODEL, WHICH ALSO MIGHT LEAK INFORMATION.
IN THE PAPER, WE MOSTLY FOCUS ON HOW THE INTERACTION WITH THE FRAME WORK AND THE MODEL MIGHT LEAGUE INFORMATION.
THE NEXT SLIDE, YOU SEE WHAT I MEAN WHEN I TALK ABOUT INFORMATION.
IT'S LIKE HOW YOU WANT TO QUANTIFY THE LEAKAGE.
WE USE THE SIMILAR APPROACH TO HONGYAN'S WORK.
SO GIVEN THE EXPLANATION, CAN AN ADVERSARY TELL IF A DATA POINT IS IN THE TRAINING SET OR NOT.
IF YOU HAVE A BACKGROUND CRYPTOGRAPHY, YOU COULD FORMULATE THIS AS A GAME AND AN ADVERSARY WOULD WIN IF HE COULD DISTINGUISH TWO EXPLANATIONS.
SO IN THE SETTING WE HAVE AN ADVERSARY.
THE ADVERSARY HAS A DATA RECORD.
GIVES IT TO THE MODEL AND GIVES BACK A PREDICTION AND EXPLANATION.
IF THE ADVERSARY WINS THE GAME, HE CAN TELL WHETHER OR NOT THE TRAINING

POINT WAS USED.
THE NEXT SLIDE.
I WANT TO SPEND A LITTLE TIME SHOWING YOU HOW THESE EXPLANATIONS MIGHT LOOK LIKE.
WE FOCUSED ON OUR WORK MOSTLY ON ATTRIBUTE BASED EXPLANATIONS.
IF YOU HAVE A CLASSIFICATION TO ASK FOR IMAGES, THE KEY ON THE LEFT, THE CLASSIFICATION TASK IS FIGURING OUT THE MOOD OF THE PHRASE.
THE EXPLANATION MADE MIGHT HIGHLIGHT PARTS OF THE PHRASE.
THE EYES WERE IMPORTANT TO PROTECT THE MOOD OF THE PERSON ON THE LOWER SIDE.
THE EYEBROWS WERE DETERMINE TO PROTECTING THE MOOD.
YOU ALSO SEE THERE'S A LOT OF FLICKERING.
THESE EXPLANATION METHODS ARE FAR FROM PERFECT.
ON MORE DATA, AN EXPLANATION METHOD ON THE RIGHT, MIGHT SAY, OKAY, YOU WOULD HAVE GOTTEN THE LOAN IF YOUR INCOME WAS HIGHER.
THE INCOME WAS THE MOST IMPORTANT FEATURE F YOU WANT TO HAVE A THEORETICAL INTUITION FOR THESE THESE EXPLANATIONS WORK, THE GRADIENT TELLS YOU HOW THE OUTPUT CHANGES WHEN YOU CHANGE THE INPUT.
SO THE NEXT SLIDE, YOU SEE KIND OF THE RESULT.
SIMILAR TO HONGYAN, I'M NOT GOING TO GO INTO DETAIL ABOUT HOW IT WORKS.
IF YOU'RE INTERESTED, IT'S IN THE PAPER.
WE DEMONSTRATED ON SEVERAL DATA SETS THAT AN ADVERSARY WITH ACCESS TO THE EXPLANATIONS CAN FIGURE OUT WHETHER OR NOT A POINT WAS USED FOR TRAINING AND HE CAN DO THIS BETTER THAN GUESSING.
SO ON THE FINAL SLIDE, LET ME CONCLUDE.
WHAT SHOULD YOU TAKE AWAY FROM MY TALK?
FIRST, WE HAVE DEMONSTRATED THAT MODEL EXPLANATIONS CAN LEAK MEMBERSHIP INFORMATION.
THE OVERALL GOAL SEEMS TO BE THAT WE WANT TRUSTWORTHY MACHINE.
WE NEED PRIVACY FOR TRUSTWORTHY MACHINERY TO WORK.
ACADEMIA HAS REACTED AND LIKE THERE ARE LOTS OF EXPLANATION FRAME WORKS OUT THERE AND NEW ONES ARE PROPOSED EVERY WEEK, I WANT TO SAY.
SO IT'S VERY LIKELY THAT THERE WILL BE USER PHASING EXPLAINABLE AND MACHINERY FRAME WORKS IN THE FUTURE.
RIGHT NOW, THE BIG COMPANIES THAT GIVE PROGRAMS TO LIKE PROGRAMMERS ALREADY INCLUDE EXPLAINABILITY TOOLS IN THEIR FRAME WORKS.
SO I HOPE THAT BOTH DEVELOPERS AND REGULATORS HAVE THE PRIVACY IMPLICATIONS IN MIND WHEN THEY ARE DESIGNING EXPLANATION METHODS.
IF YOU HAVE QUESTIONS THAT GO BEYOND, YOU CAN REACH ME AT THE E-MAIL ADDRESS AND LINKED TO THE PAPER ON THE BOTTOM OF THE SLIDE.
>> THANK YOU VERY MUCH, MARTIN.
AGAIN, TO ALL OF OUR OTHER PANELISTS FOR THOSE INFORMATIVE PRESENTATIONS.
LOOKING FORWARD TO HEARING MORE IN THE DISCUSSION PORTION, WHICH WE'LL

NOW MOVE ON TO.
I REALLY HOPE TO ENGAGE IN GREAT DISCUSSION AND EXPANDING ON THE RESEARCH THAT YOU PRESENTED AND THE IMPLICATIONS OF SUCH.
THE WORK THAT WE ALL DO.
SO FIRST, I JUST WANTED TO SAY AND ASK THE QUESTION TO YOU, BASI, RESEARCH HAS SHOWN THE PRE LENS OF BIAS INCLUDING DISCRIMINATORY OUTCOMES AND MACHINE-LEARNING ALGORITHMS FOR DIFFERENT PURPOSES.
WE'VE SEEN IT FROM HEALTHCARE, TO CREDIT, BEHAVIORAL ADVERTISING DECISIONS AS YOUR PAPER SHOWED.
AND ALGORITHMIC LEGISLATION HAS BEEN PROPOSED TO MITIGATE SUCH BIAS.
SO SORT OF TO YOU FIRST, BASI.
SEEMS THAT YOU MIGHT AGREE THAT INCREASED TRANSPARENCY MIGHT BE USEFUL IN ACHIEVING FAIRNESS IN ALGORITHMS FOR ONLINE JOB ADVERTISEMENTS.
FROM YOUR TECHNICAL POINT OF VIEW, I'D BE INTERESTING IN HEARING WHAT IMPLICATIONS YOUR RESEARCH HAS ON SUCH LEGISLATION.
WOULD YOU RECOMMEND TO INCREASE ALGORITHMIC TRANSPARENCY INCLUDING IN JOB DELIVERY ALGORITHMS?
>> THAT'S A GREAT QUESTION.
TRANSPARENCY IS ONE OF THE THINGS THAT WE CALLED FOR IN OUR WORK.
THAT CAN COME IN DIFFERENT FORMS.
ONE OF THE THINGS THAT WE COMMENT IS THAT OUR PLATFORMS NEED TO PROVIDE ADDITIONAL DATA AND STATISTICS ABOUT NOT JUST ABOUT LIKE HOW ADS ARE DELIVERED BUT WHAT HAPPENS IN THE ADD TARGET PAGE.
FOR EXAMPLE, IN LINKEDIN'S CASE, THE PLATFORM DOES NOT PROVIDE A BREAKDOWN OF ADD DELIVERY BY GENDER SO WE HAVE TO RELY ON A WORK AROUND METHODOLOGY TO AUDIT HOW THE ADS ARE DELIVERED BY GENDER.
FOR EXAMPLE, ONE WAY IS LINKEDIN CAN PROVIDE BREAKDOWN OF AD DELIVERY BY SENSITIVE ATTRIBUTES.
IN FACEBOOK'S CASE, THERE'S SOME EXISTING TRANSPARENCY EFFORTS THAT HAS A PUBLIC AD LIBRARY API THAT THEY MADE AVAILABLE, WHICH IS A GOOD FIRST STEP.
BUT WE DON'T THINK IT'S ENOUGH.
LIKE I SAID, LIKE THE TARGET ADVERTISING PIPELINE IS A COMPLEX PROCESS WITH MANY STEPS.
APPARENTLY THEY PROVIDE BREAKDOWN BY AD DELIVERY, BUT PROVIDING ADDITIONAL PARTS OF THE PIPELINE WOULD BE USEFUL.
AND TO ADD ONE MORE POINT.
ANOTHER TRANSPARENCY DIRECTION THAT WE'RE THINKING ABOUT AND WE HOPE AD PLATFORMS WOULD CONSIDER IS PROVIDING AUDITING INTERFACE THAT AUDITORS CAN USE TO QUERY DIFFERENT PARTS OF THEIR ALGORITHMS TO CERTIFY THEIR FAIRNESS.
SO THAT'S ONE DIRECTION THAT WE'RE EXPLORING AS WELL.

>> THANK YOU.
TO FOLLOW UP ON THAT HONGYAN AND MARTIN, BOTH OF YOUR PAPERS SEEM THERE'S A IN LIGHT OF THE FINDINGS OF YOUR RESEARCH WHAT IMPLICATIONS DOES YOUR RESEARCH HAVE ON TRANSPARENCY LEGISLATION.
YOU THINK THERE'S WAYS TO ACHIEVE ALGORITHMIC FAIRNESS AND PROTECT THE PRIVACY OF UNDERREPRESENTED COMMUNITIES AT THE SAME TIME OR MIGHT THERE BE SOME INHERENT TRADE-OFFS WITH PRIVACY AND FAIRNESS?

>> I THINK THIS IS AN INTERESTING QUESTION.
THE ANSWER TO THAT IS ACTUALLY WE CAN'T ACHIEVE FAIRNESS AND PRIVACY AT THE SAME TIME.
FOR EXAMPLE --
[INAUDIBLE]
-- THE MODEL WILL BE FAIR.
BECAUSE IT ALWAYS GIVE THE SAME OUTPUT TO DATA POINT IN DIFFERENT GROUPS.
THE MODEL IS PRIVACY -- THE MODEL IS INDEPENDENT OF THE DATA.
MORE IMPORTANTLY, WE CAN ACHIEVE FAIRNESS AND PRIVACY WITHOUT ACURAACY OF THE MODEL.
UNFORTUNATELY SOME WORKS SHOWED THAT DIFFERENTIAL PRIVACY CAN CONFLICT WITH MANY GROUP FAIRNESS NOTIONS, INCLUDING EQUALIZED ARTS.
SO THE RESULTS SHOW THAT THE LEARNING ALGORITHM IS SISTERING DIFFERENTIAL PRIVACY, WHICH IS A VERY STRICT NOTION, THE FAIR MODELS USED BY THIS ALGORITHM IS A CONSTANT CLASSIFIER.
SO IN OTHER WORDS, IF WE WANT TO ACHIEVE ACHIEVE PURE DIFFERENTIAL PRIVACY, GROUP FAIRNESS, THERE IS A MODEL ACCURACY WE CAN GET IS NO GREATER THAN THAT OF A CONSTANT CLASSIFIER. SO WHEN WE TALK ABOUT ACHIEVE FAIRNESS AND PRIVACY AT THE SAME TIME, I THINK PROBABLY THE FIRST THING WE NEED TO DO IS RELAX OUR PRIVACY NOTION. FOR INSTANCE, SOME EXISTING WORK ACTUALLY SHOW THAT RELAXES PRIVACY REQUIREMENTS AND STUDIES DIFFERENTIALLY PRIVATE FAIR ALGORITHM WITH RESPECT TO APPROXIMATE DPK WHICH SHOWS THAT DP, DIFFERENTIALLY PRIVATE ALGORITHM CAN'T OUTPUT A MODEL THAT ACHIEVE GOOD ACCURACY, AND FAIRNESS AT THE SAME TIME. SO I PERSONALLY THINK, STAY QUITE OPTIMISTIC. I ABOUT BELIEVE ACCURACY APPROXIMATES FAIRNESS, BUT NEEDS FURTHER FROM THE RESEARCH COMMUNITIES.
>> THANK YOU, "AMERICA MARTIN, DO YOU HAVE FURTHER ON THAT?
>> I WANT TO FOCUS TON POSITIVE. LIKE CURRENTLY I DON'T THINK THERE'S AN INHERENT RATE OF EXPENDABILITY AND PRIVACY. AND THIS IS LIKE IF YOU QUERY ABOUT THE PRIVACY OF THE TRAINING DATA AND YOU WANT TO EXPLAIN THE MODEL, THE ONLY THING YOU KIND OF NEED TO CURRENTLY IS YOUR MODEL EXPIRED. SO IF YOU HAVE A PRIVATE MODEL AND YOUR ONLY CONTEXT WITH THE MODEL YOU WOULD HAVE A PRIVATE EXPLANATION. THIS IS GOOD NOTE. ON THE BAD SIDE, IN OUR WORK, ON SOME HINTS THAT THE PRIVACY RISK FOR MINORITIES

MIGHT ACTUALLY BE HIGHER THAN FOR THE MAJORITY CLASS. SO THE PRIVACY RISK THROUGH EXPLANATIONS ON MINORITIES MIGHT BE HIGHER THAN MAJORITIES, AND THAT'S KIND OF PROBLEMATIC. BECAUSE IT IS KIND OF EXACTLY THE PEOPLE YOU WANT THE EXPLANATION FOR BECAUSE THEY ARE MOST LIKELY TO BE THE ONES WHO ARE DISCRIMINATED. SO THAT'S THE BAD PART. AND THE OTHER PART OF BAD NEWS IN FOLLOW UP VIEW TO MINE, THERE IS ACTUALLY SOME INDICATION THAT IT'S HARDER TO EXPLAIN PRIVATE MODELS. SO HOW DO YOU MAKE A MODEL PRIVATE? YOU INTRODUCE NOISE. AND THIS NOISE KIND OF IN A VERY WISHYWISHY-WASHY LEVEL IT IS COUNTERINTUITIVE. IF YOU INTRODUCE NOISE IT MAKES THE MODEL MORE IMPLICATE COMPLICATED AND NOW IT'S HARDER TO UN. SO YEAH I DON'T THINK THERE'S A FUNDAMENTAL TRADEOFF BUT THERE IS STILL WORK TO DO TO GET IT DONE.
>> THANK YOU FOR THAT. GOING BACK TO YOU BASI, SPECIFICALLY FOR GENDER DISCRIMINATION IN JOB ADVERTISEMENT AD DELIVERY WHEN PLATFORMS ARE NOT TRANSPARENT ABOUT THEIR ARE ALGORITHMS. DO YOU THINK OTHER MODELS COULD BE USED FOR OTHER FORMS OF DISCRIMINATION SUCH AS RACE OR SEXUAL ORIENTATION OR COULD IT IS BE USED FOR MACHINE ALGORITHMS, SERVED FOR ADS FOR OTHER TYPES OF THINGS SUCH AS CREDIT OR HOUSING OR EVEN ALGORITHMS DOLLAR USED TO ASSIST IN CREDIT OR HOUSING DECISIONS AND IF SO DO YOU THINK THERE WOULD BE ANY LIMITATIONS FOR USING SUCH METHODS?
>> YEAH, THAT'S A GREAT QUESTION. THE FIRST ANSWER IS YES. WE'D BE ABLE TO EXTEND THIS METHODOLOGY --
>> I THINK DID BASI FREEZE? OKAY, WE'LL GO MAYBE TO THE NEXT QUESTION AND HOPEFULLY WE CAN HEAR FROM HIM ON THAT BECAUSE I'D REALLY BE --
>> AM I BACK?
>> YES YOU'RE BACK. YOU FROZE FOR A MOMENT.
>> OKAY, GREAT, WE USED VOTER DATA FROM NORTH CAROLINA TO CEASE AN AUDIENCE WHERE WE KNOW BOTH THE GENDER AND THE LOCATION. BECAUSE LINKEDIN PROVIDES BREAKDOWN BY LOCATION AND WE USE THAT AS A FROIX TO CALCULATE THE GENDER BREAKDOWN. SIMILARLY, THE GENDER FIELDS INCLUDE OTHER THINGS LIKE RACE AND AGE. SO WE WOULD BE ABLE TO USE THOSE ABOUT THE AUDIT FOR DISCRIMINATION BY RACE AND AGE. BUT THE CAVEAT IS THAT LIKE I MENTIONED IN THE TALK WE WOULD NEED TO FIND A PAIR OF JOB POSITION WEST SIMILAR REQUIREMENTS BUT THERE IS AN IMBALANCE BY RACE OR AGE OR OTHER SENSITIVE ATTRIBUTES THAT WE'RE INTERESTED IN. AND IN RESPONSE TO YOUR QUESTION ABOUT THE LIMITATION, ONE OF THE MAIN LIMITATIONS WE TALK ABOUT IN THE PAPER COMES FROM USING LOCATION AS A FROIX TO SUBSTITUTE GENDER BECAUSE FOR EXAMPLE PEOPLE MIGHT MOVE BETWEEN DIFFERENT LOCATIONS OR THE DATA MIGHT BE OUTDATED. SO THERE IS SOME ERROR THAT ACCOMMODATION FROM THAT, AND THE OTHER LIMITATION IS THE COAST INVOLVED IN RUNNING THESE ADS, WE RUN OR EXPERIMENTAL MULTIPLE AUDIENCES AND ALSO DIFFERENT JOB CATEGORIES SEEKING CONFIDENCE IN OUR RESULTS AND THE COSTS CAN EASILY ADD UP IF WE WANT TO GAIN MORE CONFIDENCE IN OUR RESULTS. SO YES. THERE ARE THOSE CAVEATS. BUT YES, OUR METHOD CAN BE

EXTENDED.
>> THANK YOU. AGAIN, YOUR PAPER COVERS ONE SCENARIO WHERE FAIRNESS CAN CONFLICT WITH PRIVACY, SPECIFICALLY GROUP FAIRNESS AS YOU WERE DISCUSSING EARLIER ON EQUALIZED ODDS. ARE THERE OTHER WAYS THAT YOU THINK PRIVACY AND FAIRNESS CAN CONFLICT IN MACHINE LEARNING ALGORITHMS THAT YOU HAVEN'T ALREADY DISCUSSED?
>> YES, THANKS FOR THE QUESTION. I THINK FAIRNESS AND PRIVACY COULD CONFLICT WITH EACH OTHER IN OTHER SCENARIOS. ONE SCENARIO THAT DRAWS A LOT OF ATTENTION IS WHEN WE CARE ABOUT THE PRIVACY WITH RESPECT TO THE SENSITIVE ATTRIBUTES SUCH AS RACE, GENDER. SO FREQUENT, JDPR RESTRICTS THE RACIAL DATA COLLECTION FROM CUSTOMERS. SO IT PROTECT THE PRIVACY WITH RESPECT TO THE SENSITIVE ATTRIBUTES BUT ACTUALLY IT IS RACE IS A BIG ISSUE FOR TRAINING OF A FAIR MODEL. BECAUSE RESEARCHERS HAVE FOUND HAD A FAIRNESS CAN ONLY BE ACHIEVED THROUGH AWARENESS. SO FOR EXAMPLE, IF YOU WANT TO BUILD A GENDER FAIR CLASSIFIER AND YOU EXCLUDE THE GENDER ATTRIBUTES, IT DOES NOT PROVIDE -- IT DOES NOT GUARANTEE TO HAVE -- TO PROVIDE FAIRNESS AND IT WILL HURT THE ACCURACY OF THE MODEL. SO IT IS BECAUSE THAT THERE ARE MANY OTHER FEATURES THAT ARE WELL CORRELATED WITH YOUR AGENDA. FOR INSTANCE, WE CAN'T MAKE A GOOD GUESS ABOUT INDIVIDUALS GENDER BY KNOWING THEIR FAVORITE SONGS AND FAVORITE COLORS. SO IN THIS CASE, THE GENDER BLOOD MODEL MAY DISCRIMINATE AGAINST MALES OR FEMALES BY DISCRIMINATING AGAINST THE PEOPLE WHO LIKE A PARTICULAR SONG. SO THIS ALLOWING THE COLLECTION OF THE SENSITIVE ATTRIBUTES FOR PROTECTING PRIVACY INDEED RAISES A PROBLEM FOR FAIRNESS. AND ANOTHER IMPORTANT SCENARIO IS WHEN PRIVACY IS ACHIEVED BY ADDING NOISE TO INDIVIDUAL'S DATA. SO THE MODEL CAN ONLY SEE THE NOISY VERSION OF THE INDIVIDUAL'S DATA. ACTUALLY, IN THIS CASE, SOME RESEARCHERS ALSO FOUND THAT THE RESULTS ALLOCATION DECISIONS MADE ON THIS NOISY DATA CAN DISPROPORTIONATELY AFFECT SOME SUBGROUPS. SO OVERALL THERE ARE A LOT OF WAYS PRIVACY CAN CONFLICT WITH FAIRNESS IN MARBLING ANY TASK. BASICALLY IT TELLS US WHEN WE ASK FOR PRIVACY AND FAIRNESS WE REALLY NEED TO THINK OF BOTH OF THEM AT THE SAME TIME BECAUSE IT CAN REALLY AFFECT EACH OTHER.
>> GOOD THANK YOU FOR THAT. MARTIN, THROWING IT TO YOU. YOUR PAPER FOCUSES ON THE PRIVACY ASPECTS OF DATA, SPECIFICALLY STATE HEERLDZ AND THE DEPLOYMENT OF MACHINE LEARNING MODEL EXPLANATION TOOLS. ARE THERE OTHER STAKEHOLDERS INCLUDING THOSE FOR EXAMPLE INVOLVED IN THE DESIGN OR DEVELOPMENTS OF MACHINE LEARNING FOR MODEL EXPLANATION TOOLS THAT YOU THINK MIGHT SEE THEIR PRIVACY ERODED?
>> YES, THANKS FOR QUESTION. SO I HINTED AT THIS IN THE TALK A LITTLE BIT. SO I THINK THE BIGGEST HURDLE FOR EXPLANATION, IS NOT SO MUCH THE PRIVACY OF THE DATA, IT'S THE PRIVACY OF THE MODEL AND THE FACT THAT WHOEVER EQUATES THE MODEL WANTS TO PIRATE. THERE IS ALSO RESEARCH OUT THAT DEMONSTRATES DID YOU SEE ENOUGH PREDICTIONS OF THE MODEL YOU CAN

REPRODUCE IT. AND IF YOU EXPLAIN THESE PREDICTIONS, IT JUST BECOMES EASIER TO REPRODUCE THE MODEL. SO I THINK THE COMPANIES MIGHT HAVE AN INTEREST IN NOT RELEASING EXPLANATIONS BECAUSE IT MAKES IT EASIER TO KIND OF EXTRACT THE MODELS. AND THEN JUST LIKE COPY THE MODELS. SO THIS IS KIND OF THE ONE BIG STAKEHOLDER THAT MIGHT SEE THEIR PRIVACY AFFECTED.
>> I KIND OF WANT TO GO BACK TO SORT OF LIKE YOU, HONGYAN AND MARTIN SORT OF ABOUT THE CLEKS OF DATA AND MAYBE THE COLLECTION OF SENSITIVE ATTRIBUTES VERSUS WHEN YOU SPLIET DUTY WITH ADDED NOISE. AND YOU KNOW I KNOW THERE'S BEEN SOME TECHNOLOGY EXPERTS WHO ADVOCATE FOR THE NEED TO HAVE MORE COLLECTION OF DATA SO YOU NEED MORE INFORMATION ON PROTECTED CHARACTERISTICS OF UNDERREPRESENTED COMMUNITIES AND THINGS LIKE THAT, WHILE OTHERS MIGHT SUGGEST THAT IT'S POSSIBLE TO MITIGATE ALGORITHMIC BIAS WITHOUT COLLECTING DEMOGRAPHIC OR PROXY DATA, SUCH AS USING SIMULATED DATA WHERE YOU'VE ADDED IN NOISE. THIS IS A QUESTION FOR ALL OF OUR PANELIST, WOULD YOU RECOMMEND AND DO YOU THINK THAT THERE ARE ANY PRIVACY RISKS OF AN APPROACH YOU WOULD RECOMMEND?
>> THANKS FOR THE QUESTION. I THINK THIS IS A VERY INTERESTING QUESTION. SO FIRST OFF, I WOULD LIKE TO MENTION THAT THE TRADEOFF IS IN FAIRNESS, I MENTIONED IT BEFORE, EVEN NUMBER OF SAMPLES. SO THERE IS A HARDER ARE TAIDOFF IN PRIVACY AND FAIRNESS EVEN WITH A LIMITED NUMBER OF SAMPLES. IN PRACTICE, IF WE HAVE MORE DATA FROM THE DISTRIBUTION THEN THE PRIVACY RISK WILL BE REDUCED. IN FACT IN OUR PAPER WE ANALYZE THERE EFFECT OF MODE DEFECT COLLECTION, ON THE PRIVACY AND FAIRNESS. ACTUALLY WHEN THERE IS MORE DATA FROM THE OTHER REPRESENTED GROUP, THE DATA IS MORE BALANCED. IN THIS CASE IS STANDARD MODEL IS ALSO LESS BIASED. AS A CONSEQUENCE THE PRIVACY COST OF ACHIEVING FAIRNESS IS ALSO REDUCED. SO IN OTHER WORDS, COLLECTION FROM THE OTHER REPRESENTATIVED GROUP CAN HELP TO REDUCE THE COST OF ACHIEVING FAIRNESS. AND ANOTHER THING YOU TALK ABOUT IS SIMILAR OF THE DATA. I THINK IT'S A I HAVE INTERESTING QUESTION BECAUSE BETTER TO USE THIS KIND OF TECHNIQUE SO WE MUST MAKE SURE THAT THIS SIMILAR DATA IS PRIVACY PRESERVING. BECAUSE NORMALLY WE USE THIS SIMULATED DATA BASED ON SOME PRIVATE DATA. SO THIS SIMULATED DATA MAY QUAIN SENSITIVE DATA ABOUT THE ORIGINAL. SO IF WE WANT TO USE THIS KIND OF TECHNIQUES WE MUST MAKE SURE THAT THE INDIVIDUAL INFORMATION WON'T BE MIXED THROUGH THIS SIMULATED DATA. AND ANOTHER QUALITY THAT WE WANT TO MAKE SURE THAT ANY FAIRNESS GUARANTEE A MODEL PROVIDES ON THIS SIMULATED DATA SHOULD ALSO HOLD APPROXIMATELY ORIGINAL DATA SET OTHER DISTRIBUTION WOULD CARE ABOUT. SO SIMULATED DATA SATISFY THESE TWO REQUIREMENTS WOULD BE A VERY INTERESTING THING WE SHOULD LOOK AT, IN MY OPINION THIS IS A GOOD RESEARCH DIRECTION WE SHOULD DEFINITELY LOOK AT.
>> I'LL BE LOOKING FORWARD TO THAT RESEARCH. BASI DO YOU HAVE ANY RESPONSES?
>> I WANT TO ADD SOMETHING TO OHONGYAN'S CIVIL LATED DATA. THEY NEED ACCESS TO THE DATA TO KIND OF HAVE A CONTEXT AND THEN EXPLAIN IT IN THE

CONTEXT IN DIFFERENT CONTEXT. DEFINITELY EXPECT YOU MIGHT NEED DIFFERENT EXPLANATIONS. NOW IF YOU ONLY HAVE SIMULATED DATA, YOUR EXPLANATION TO BE PRIVACY PRESERVING SHOULD BE ON THE SIMULATED DATA AND THERE IS SLIGHTLY A DIFFERENT CONTEXT DHAN THE ORIGINAL DATA. SO YOU NEED TO KIND OF ENSURE THAT THE EXPLANATIONS YOU GAIN THE SKIM LATED DATA ARE ACTUALLY LIKE USEFUL IN THE REAL WORLD THAT YOU THEN BASE IT ON REAL DATA. SO I WANT TO ADD THIS TO THE LIST OF HONGYAN'SN'S CRITERIA. IT SHOULD BE EXPLAINABLE IDEALLY.
>> THAT MAKES SENSE. AND I KNOW WE'RE ONLY HAVE A FEW

;
; 07/27/21 5:04 AM
;
;;;;FTC 210727

IN FACEBOOK'S CASE, THERE ARE SOME EXISTING TRANSPARENCY EFFORTS SUCH AS A PUBLIC AD LIBRARY API THAT THEY MADE AVAILABLE WHICH IS A GOOD FIRST STEP.
BUT WE DON'T THINK IT'S ENOUGH. THERE IS LIKE I SAID, LIKE THE TARGET ADVERTISING PIPELINE IS LEARNING ALGORITHM IS SATISFIED, VERY STRICT DIFFERENTIAL PRIVACY NOTION THEN THE FAIR MODELS OUTPUTTED BY THIS ALGORITHM IS CONSTANT CLASSIFIER.
SO IN OTHER WORDS, IF WE WANT TO ACHIEVE PURE DIFFERENTIAL PRIVACY, GROUP FAIRNESS, THERE IS A MODEL ACCURACY WE CAN GET IS NO GREATER THAN THAT OF A CONSTANT CLASSIFIER.
SO WHEN WE TALK ABOUT ACHIEVE FAIRNESS AND PRIVACY AT THE SAME TIME, I THINK PROBABLY THE FIRST THING WE NEED TO DO IS RELAX OUR PRIVACY NOTION.
FOR INSTANCE, SOME EXISTING WORK ACTUALLY SHOW THAT RELAXES PRIVACY REQUIREMENTS AND STUDIES

DIFFERENTIALLY PRIVATE FAIR ALGORITHM WITH RESPECT TO APPROXIMATE DPK WHICH SHOWS THAT DP, DIFFERENTIALLY PRIVATE ALGORITHM CAN'T OUTPUT A MODEL THAT ACHIEVE GOOD ACCURACY, AND FAIRNESS AT THE SAME TIME.
SO I PERSONALLY THINK, STAY QUITE OPTIMISTIC.
I ABOUT BELIEVE ACCURACY APPROXIMATES FAIRNESS, BUT NEEDS FURTHER FROM THE RESEARCH COMMUNITIES.
>> THANK YOU, MARTIN, DO YOU HAVE FURTHER ON THAT?
>> I WANT TO FOCUS TON POSITIVE. LIKE CURRENTLY I DON'T THINK THERE'S AN INHERENT RATE OF EXPENDABILITY AND PRIVACY.
AND THIS IS LIKE IF YOU QUERY ABOUT THE PRIVACY OF THE TRAINING DATA AND YOU WANT TO EXPLAIN THE MODEL, THE ONLY THING YOU KIND OF NEED TO CURRENTLY IS YOUR MODEL EXPIRED.
SO IF YOU HAVE A PRIVATE MODEL AND YOUR ONLY CONTEXT WITH THE MODEL YOU WOULD HAVE A PRIVATE EXPLANATION.
THIS IS GOOD NOTE.
ON THE BAD SIDE, IN OUR WORK, ON SOME HINTS THAT THE PRIVACY RISK FOR MINORITIES MIGHT ACTUALLY BE HIGHER THAN FOR THE MAJORITY CLASS.
SO THE PRIVACY RISK THROUGH EXPLANATIONS ON MINORITIES MIGHT BE HIGHER THAN MAJORITIES, AND THAT'S KIND OF PROBLEMATIC.
BECAUSE IT IS KIND OF EXACTLY THE PEOPLE YOU WANT THE EXPLANATION FOR BECAUSE THEY ARE MOST LIKELY TO BE THE ONES WHO ARE DISCRIMINATED.

SO THAT'S THE BAD PART.
AND THE OTHER PART OF BAD NEWS IN FOLLOW UP VIEW TO MINE, THERE IS ACTUALLY SOME INDICATION THAT IT'S HARDER TO EXPLAIN PRIVATE MODELS.
SO HOW DO YOU MAKE A MODEL PRIVATE?
YOU INTRODUCE NOISE.
AND THIS NOISE KIND OF IN A VERY WISHY-WASHY LEVEL IT IS COUNTERINTUITIVE.
IF YOU INTRODUCE NOISE IT MAKES THE MODEL MORE IMPLICATE COMPLICATED AND NOW IT'S HARDER TO UN.
SO YEAH I DON'T THINK THERE'S A FUNDAMENTAL TRADEOFF BUT THERE IS STILL WORK TO DO TO GET IT DONE.
>> THANK YOU FOR THAT.
GOING BACK TO YOU BASI, SPECIFICALLY FOR GENDER DISCRIMINATION IN JOB ADVERTISEMENT AD DELIVERY WHEN PLATFORMS ARE NOT TRANSPARENT ABOUT THEIR ARE ALGORITHMS.
DO YOU THINK OTHER MODELS COULD BE USED FOR OTHER FORMS OF DISCRIMINATION SUCH AS RACE OR SEXUAL ORIENTATION OR COULD IT IS BE USED FOR MACHINE ALGORITHMS, SERVED FOR ADS FOR OTHER TYPES OF THINGS SUCH AS CREDIT OR HOUSING OR EVEN ALGORITHMS DOLLAR USED TO ASSIST IN CREDIT OR HOUSING DECISIONS AND IF SO DO YOU THINK THERE WOULD BE ANY LIMITATIONS FOR USING SUCH METHODS?
>> YEAH, THAT'S A GREAT QUESTION.
THE FIRST ANSWER IS YES.
WE'D BE ABLE TO EXTEND THIS

METHODOLOGY --
>> I THINK DID BASI FREEZE?
OKAY, WE'LL GO MAYBE TO THE NEXT QUESTION AND HOPEFULLY WE CAN HEAR FROM HIM ON THAT BECAUSE I'D REALLY BE --
>> AM I BACK?
>> YES YOU'RE BACK.
YOU FROZE FOR A MOMENT.
>> OKAY, GREAT, WE USED VOTER DATA FROM NORTH CAROLINA TO CEASE AN AUDIENCE WHERE WE KNOW BOTH THE GENDER AND THE LOCATION.
BECAUSE LINKEDIN PROVIDES BREAKDOWN BY LOCATION AND WE USE THAT AS A FROIX TO CALCULATE THE GENDER BREAKDOWN.
SIMILARLY, THE GENDER FIELDS INCLUDE OTHER THINGS LIKE RACE AND AGE.
SO WE WOULD BE ABLE TO USE THOSE ABOUT THE AUDIT FOR DISCRIMINATION BY RACE AND AGE.
BUT THE CAVEAT IS THAT LIKE I MENTIONED IN THE TALK WE WOULD NEED TO FIND A PAIR OF JOB POSITION WEST SIMILAR REQUIREMENTS BUT THERE IS AN IMBALANCE BY RACE OR AGE OR OTHER SENSITIVE ATTRIBUTES THAT WE'RE INTERESTED IN.
AND IN RESPONSE TO YOUR QUESTION ABOUT THE LIMITATION, ONE OF THE MAIN LIMITATIONS WE TALK ABOUT IN THE PAPER COMES FROM USING LOCATION AS A FROIX TO SUBSTITUTE GENDER BECAUSE FOR EXAMPLE PEOPLE MIGHT MOVE BETWEEN DIFFERENT LOCATIONS OR THE DATA MIGHT BE OUTDATED.
SO THERE IS SOME ERROR THAT ACCOMMODATION FROM THAT, AND THE OTHER LIMITATION IS THE COAST

INVOLVED IN RUNNING THESE ADS,
WE RUN OR EXPERIMENTAL MULTIPLE
AUDIENCES AND ALSO DIFFERENT JOB
CATEGORIES SEEKING CONFIDENCE IN
OUR RESULTS AND THE COSTS CAN
EASILY ADD UP IF WE WANT TO GAIN
MORE CONFIDENCE IN OUR RESULTS.
SO YES.
THERE ARE THOSE CAVEATS.
BUT YES, OUR METHOD CAN BE
EXTENDED.
>> THANK YOU.
AGAIN, YOUR PAPER COVERS ONE
SCENARIO WHERE FAIRNESS CAN
CONFLICT WITH PRIVACY,
SPECIFICALLY GROUP FAIRNESS AS
YOU WERE DISCUSSING EARLIER ON
EQUALIZED ODDS.
ARE THERE OTHER WAYS THAT YOU
THINK PRIVACY AND FAIRNESS CAN
CONFLICT IN MACHINE LEARNING
ALGORITHMS THAT YOU HAVEN'T
ALREADY DISCUSSED?
>> YES, THANKS FOR THE QUESTION.
I THINK FAIRNESS AND PRIVACY
COULD CONFLICT WITH EACH OTHER
IN OTHER SCENARIOS.
ONE SCENARIO THAT DRAWS A LOT OF
ATTENTION IS WHEN WE CARE ABOUT
THE PRIVACY WITH RESPECT TO THE
SENSITIVE ATTRIBUTES SUCH AS
RACE, GENDER.
SO FREQUENT, JDPR RESTRICTS THE
RACIAL DATA COLLECTION FROM
CUSTOMERS.
SO IT PROTECT THE PRIVACY WITH
RESPECT TO THE SENSITIVE
ATTRIBUTES BUT ACTUALLY IT IS
RACE IS A BIG ISSUE FOR TRAINING
OF A FAIR MODEL.
BECAUSE RESEARCHERS HAVE FOUND
HAD A FAIRNESS CAN ONLY BE
ACHIEVED THROUGH AWARENESS.
SO FOR EXAMPLE, IF YOU WANT TO

BUILD A GENDER FAIR CLASSIFIER AND YOU EXCLUDE THE GENDER ATTRIBUTES, IT DOES NOT PROVIDE -- IT DOES NOT GUARANTEE TO HAVE -- TO PROVIDE FAIRNESS AND IT WILL HURT THE ACCURACY OF THE MODEL.
SO IT IS BECAUSE THAT THERE ARE MANY OTHER FEATURES THAT ARE WELL CORRELATED WITH YOUR AGENDA.
FOR INSTANCE, WE CAN'T MAKE A GOOD GUESS ABOUT INDIVIDUALS GENDER BY KNOWING THEIR FAVORITE SONGS AND FAVORITE COLORS.
SO IN THIS CASE, THE GENDER BLOOD MODEL MAY DISCRIMINATE AGAINST MALES OR FEMALES BY DISCRIMINATING AGAINST THE PEOPLE WHO LIKE A PARTICULAR SONG.
SO THIS ALLOWING THE COLLECTION OF THE SENSITIVE ATTRIBUTES FOR PROTECTING PRIVACY INDEED RAISES A PROBLEM FOR FAIRNESS.
AND ANOTHER IMPORTANT SCENARIO IS WHEN PRIVACY IS ACHIEVED BY ADDING NOISE TO INDIVIDUAL'S DATA.
SO THE MODEL CAN ONLY SEE THE NOISY VERSION OF THE INDIVIDUAL'S DATA.
ACTUALLY, IN THIS CASE, SOME RESEARCHERS ALSO FOUND THAT THE RESULTS ALLOCATION DECISIONS MADE ON THIS NOISY DATA CAN DISPROPORTIONATELY AFFECT SOME SUBGROUPS.
SO OVERALL THERE ARE A LOT OF WAYS PRIVACY CAN CONFLICT WITH FAIRNESS IN MARBLING ANY TASK.
BASICALLY IT TELLS US WHEN WE ASK FOR PRIVACY AND FAIRNESS WE REALLY NEED TO THINK OF BOTH OF

THEM AT THE SAME TIME BECAUSE IT
CAN REALLY AFFECT EACH OTHER.
>> GOOD THANK YOU FOR THAT.
MARTIN, THROWING IT TO YOU.
YOUR PAPER FOCUSES ON THE
PRIVACY ASPECTS OF DATA,
SPECIFICALLY STATE HEERLDZ AND
THE DEPLOYMENT OF MACHINE
LEARNING MODEL EXPLANATION
TOOLS.
ARE THERE OTHER STAKEHOLDERS
INCLUDING THOSE FOR EXAMPLE
INVOLVED IN THE DESIGN OR
DEVELOPMENTS OF MACHINE LEARNING
FOR MODEL EXPLANATION TOOLS THAT
YOU THINK MIGHT SEE THEIR
PRIVACY ERODED?
>> YES, THANKS FOR QUESTION.
SO I HINTED AT THIS IN THE TALK
A LITTLE BIT.
SO I THINK THE BIGGEST HURDLE
FOR EXPLANATION, IS NOT SO MUCH
THE PRIVACY OF THE DATA, IT'S
THE PRIVACY OF THE MODEL AND THE
FACT THAT WHOEVER EQUATES THE
MODEL WANTS TO PIRATE.
THERE IS ALSO RESEARCH OUT THAT
DEMONSTRATES DID YOU SEE ENOUGH
PREDICTIONS OF THE MODEL YOU CAN
REPRODUCE IT.
AND IF YOU EXPLAIN THESE
PREDICTIONS, IT JUST BECOMES
EASIER TO REPRODUCE THE MODEL.
SO I THINK THE COMPANIES MIGHT
HAVE AN INTEREST IN NOT
RELEASING EXPLANATIONS BECAUSE
IT MAKES IT EASIER TO KIND OF
EXTRACT THE MODELS.
AND THEN JUST LIKE COPY THE
MODELS.
SO THIS IS KIND OF THE ONE BIG
STAKEHOLDER THAT MIGHT SEE THEIR
PRIVACY AFFECTED.
>> I KIND OF WANT TO GO BACK TO

SORT OF LIKE YOU, HONGYAN AND
MARTIN SORT OF ABOUT THE CLEKS
OF DATA AND MAYBE THE COLLECTION
OF SENSITIVE ATTRIBUTES VERSUS
WHEN YOU SPLIET DUTY WITH ADDED
NOISE.
AND YOU KNOW I KNOW THERE'S BEEN
SOME TECHNOLOGY EXPERTS WHO
ADVOCATE FOR THE NEED TO HAVE
MORE COLLECTION OF DATA SO YOU
NEED MORE INFORMATION ON
PROTECTED CHARACTERISTICS OF
UNDERREPRESENTED COMMUNITIES AND
THINGS LIKE THAT, WHILE OTHERS
MIGHT SUGGEST THAT IT'S POSSIBLE
TO MITIGATE ALGORITHMIC BIAS
WITHOUT COLLECTING DEMOGRAPHIC
OR PROXY DATA, SUCH AS USING
SIMULATED DATA WHERE YOU'VE
ADDED IN NOISE.
THIS IS A QUESTION FOR ALL OF
OUR PANELIST, WOULD YOU
RECOMMEND AND DO YOU THINK THAT
THERE ARE ANY PRIVACY RISKS OF
AN APPROACH YOU WOULD RECOMMEND?
>> THANKS FOR THE QUESTION.
I THINK THIS IS A VERY
INTERESTING QUESTION.
SO FIRST OFF, I WOULD LIKE TO
MENTION THAT THE TRADEOFF IS IN
FAIRNESS, I MENTIONED IT BEFORE,
EVEN NUMBER OF SAMPLES.
SO THERE IS A HARDER ARE TAIDOFF
IN PRIVACY AND FAIRNESS EVEN
WITH A LIMITED NUMBER OF
SAMPLES.
IN PRACTICE, IF WE HAVE MORE
DATA FROM THE DISTRIBUTION THEN
THE PRIVACY RISK WILL BE
REDUCED.
IN FACT IN OUR PAPER WE ANALYZE
THERE EFFECT OF MODE DEFECT
COLLECTION, ON THE PRIVACY AND
FAIRNESS.

ACTUALLY WHEN THERE IS MORE DATA
FROM THE OTHER REPRESENTED
GROUP, THE DATA IS MORE
BALANCED.
IN THIS CASE IS STANDARD MODEL
IS ALSO LESS BIASED.
AS A CONSEQUENCE THE PRIVACY
COST OF ACHIEVING FAIRNESS IS
ALSO REDUCED.
SO IN OTHER WORDS, COLLECTION
FROM THE OTHER REPRESENTATIVED
GROUP CAN HELP TO REDUCE THE
COST OF ACHIEVING FAIRNESS.
AND ANOTHER THING YOU TALK ABOUT
IS SIMILAR OF THE DATA.
I THINK IT'S A I HAVE
INTERESTING QUESTION BECAUSE
BETTER TO USE THIS KIND OF
TECHNIQUE SO WE MUST MAKE SURE
THAT THIS SIMILAR DATA IS
PRIVACY PRESERVING.
BECAUSE NORMALLY WE USE THIS
SIMULATED DATA BASED ON SOME
PRIVATE DATA.
SO THIS SIMULATED DATA MAY QUAIN
SENSITIVE DATA ABOUT THE
ORIGINAL.
SO IF WE WANT TO USE THIS KIND
OF TECHNIQUES WE MUST MAKE SURE
THAT THE INDIVIDUAL INFORMATION
WON'T BE MIXED THROUGH THIS
SIMULATED DATA.
AND ANOTHER QUALITY THAT WE WANT
TO MAKE SURE THAT ANY FAIRNESS
GUARANTEE A MODEL PROVIDES ON
THIS SIMULATED DATA SHOULD ALSO
HOLD APPROXIMATELY ORIGINAL DATA
SET OTHER DISTRIBUTION WOULD
CARE ABOUT.
SO SIMULATED DATA SATISFY THESE
TWO REQUIREMENTS WOULD BE A VERY
INTERESTING THING WE SHOULD LOOK
AT, IN MY OPINION THIS IS A GOOD
RESEARCH DIRECTION WE SHOULD

DEFINITELY LOOK AT.
>> I'LL BE LOOKING FORWARD TO THAT RESEARCH.
BASI DO YOU HAVE ANY RESPONSES?
>> I WANT TO ADD SOMETHING TO OHONGYAN'S CIVIL LATED DATA.
THEY NEED ACCESS TO THE DATA TO KIND OF HAVE A CONTEXT AND THEN EXPLAIN IT IN THE CONTEXT IN DIFFERENT CONTEXT.
DEFINITELY EXPECT YOU MIGHT NEED DIFFERENT EXPLANATIONS.
NOW IF YOU ONLY HAVE SIMULATED DATA, YOUR EXPLANATION TO BE PRIVACY PRESERVING SHOULD BE ON THE SIMULATED DATA AND THERE IS SLIGHTLY A DIFFERENT CONTEXT DHAN THE ORIGINAL DATA.
SO YOU NEED TO KIND OF ENSURE THAT THE EXPLANATIONS YOU GAIN THE SKIM LATED DATA ARE ACTUALLY LIKE USEFUL IN THE REAL WORLD THAT YOU THEN BASE IT ON REAL DATA.
SO I WANT TO ADD THIS TO THE LIST OF HONGYAN'S CRITERIA.
IT SHOULD BE EXPLAINABLE IDEALLY.
>> THAT MAKES SENSE.
AND I KNOW WE'RE ONLY HAVE A FEW MINUTES LEFT AND I DON'T KNOW IF YOU WANTED TO ADD ANYTHING ON THAT BASI OR YOU KNOW I WOULD REALLY BE INTERESTED IN HEARING FROM ALL OF OUR PANELISTS ON OUR LAST FEW MINUTES IF YOU HAD ANY THOUGHTS ON HOW YOU THINK POLICY MAKERS OR LAW ENFORCEMENT AGENCIES LIKE THE FTC CAN HELP MITIGATE ALGORITHMIC BIAS AND ADD DELIVERY ALGORITHMS USED BY PLATFORMS OR ANY OTHER MACHINE LEARNING TOOLS WHILE PROTECTING CONSUMERS' PRIVACY INTERESTS.

I DON'T KNOW WHO WOULD LIKE TO BEGIN.
HOW ABOUT YOU, BASI?
>> I CAN START, YEAH.
SO LIKE I MENTIONED IN THE TALK.
THE TECHNICAL EVIDENCE THAT WE SHOW SHOWS THAT THE WAY AD PLATFORMS IN DELIVERY IS SIGNIFICANT IN THAT REGULATIONS AND POLICIES SHOULD TAKE THAT INTO ACCOUNT.
I THINK A GOOD FIRST STEP WOULD BE FOR TECHNICAL LEGAL AND POLICY EXPERTS TO BE IN THE SAME ROOM AND LOOK AT THE TECHNICAL EVIDENCE FROM BOTH OUR WORK AND OTHER PRIOR AUDIT FINDINGS TO SEE WHETHER THOSE TECHNICAL AUDITS, THE FINDINGS ARE ENOUGH TO DPOAR OR ENACT NEW POLICIES, AND IF NOT IF THAT'S NOT THE CASE, WHAT ARE ADDITIONAL TECHNICAL CONTRIBUTIONS WOULD BE USEFUL, YEAH, TO INFORM LIKE DPEECH POLICIES THAT THUS FAR ARE OUR RECOMMENDATIONS.
>> ANYONE ELSE IN THE LAST FEW SECONDS?
WE HAVE ABOUT A MINUTE.
>> OKAY, THE WORST CASE I SEE IS DID BEAM PEOPLE LOOK AT OUR WORK AND SAY OH THIS TRANSPARENCY HAS PRIVACY IMPLICATION SO WE SHUT DOWN AND HAVE LESS TRANSPARENCY.
SO I ACTUALLY 30 WE HAVE MORE WORK LIKE BASI'S.
AND I THINK THE FTC CAN HELP.
OF COURSE IT CAN REGULATE WHO HAS ACCESS TO THIS TRANSPARENCY TOOLS AND LIKE IF AUDITORS HAVE ACCESS AND LIKE BEING TRUSTED AUDITORS HAVE ACCESS THINK THERE'S LITTLE PRIVACY RISK, THE PRIVACY RISK COMES FROM LIKE

EVERYBODY HAVING ACCESS.
SO IF YOU KIND OF CAN ENSURE
THAT THE RIGHT PEOPLE GET ACCESS
AND MORE PEOPLE LIKE BASI HAVE
ACCESS THAT WOULD BE GOOD.
>> OKAY, THANK YOU, I MEAN THIS
HAS BEEN A VERY INTERESTING
DISCUSSION.
I WANT DO THANK AGAIN ALL OF OUR
PANELISTS FOR THEIR AMAZING
PRESENTATIONS, THIS AWESOME
DISCUSSION.
WE HOPE EVERYONE WILL STICK
AROUND.
WE HAVE ANOTHER PRESENTATION ON
AUDITING MACHINE ALGORITHMS FOR
BIAS.
THANK ALL OF OUR PANELISTS AND I
APPRECIATE EVERYONE FOR STICKING
AROUND.
>> THANK YOU.
§§ §§ §§ §§
>> GOOD MORNING, MY NAME IS
LERONE BANKS, IT'S MY PLEASURE
TO PRESENT ZIAD OBERMEYER FROM
U.C. BERKELEY, PRACTICAL STEPS
ORGANIZATIONS CAN TAKE TO
IDENTIFY BIAS IN THEIR
APPLICATIONS.
PLEASE SEND YOUR QUESTIONS VIA
TWISHT OR E-MAIL AND WE'LL GET
TO THEM AFTER THE PRESENTATION.
WITH THAT, GIVE YOUR DEACONS TO
ZIAD OBERMEYER.
>> THANK YOU, I'LL TALK ABOUT
WORK WITH ANY CO-AUTHORS AND THE
REST OF MY TEAM, WE'VE BEEN
DOING TO TRY TO DIAGNOSE AND FIX
ALGORITHMIC BIAS OVER THE PAST
COUPLE OF YEARS.
CASE STUDY AND TRANSITION TO THE
PRACTICAL STEPS THAT I THINK
WE'VE LEARNED CAN BE REALLY,
REALLY EFFECTIVE FOR THE SCHOOL

FIXING ALGORITHMIC BIAS.
I'M GOING DO TRY TO WRAP THAT UP IN 15 MINUTES, MOSTLY BECAUSE I REALLY LIKE CHATTING WITH LERONE AND I LIKE CHATTING ABOUT THE LINKS BETWEEN ALGORITHMIC BIAS AND PRESENTATION.
LET'S WORK THROUGH A CASE STUDY.
I THINK THIS IS AN EXAMPLE I LEARNED A LOT FROM, COMING FROM A PAPER WE PUBLISHED TWO YEARS AGO IN SCIENCE AND IT WORKS THROUGH A CASE STUDY IN HEALTH OF HEALTH SYSTEMS THAT ARE TRYING TO TARGET EXTRA HELP TO PATIENTS WHO NEED IT.
SO ALL THROUGHOUT OUR HEALTH SYSTEM THERE ARE THESE POCKETS OF COMPLEX CHRONICALLY ILL PATIENTS AND THOSE PATIENTS ARE HAVING A VERY BAD EXPERIENCE WITH THEIR CARE, THEY'RE EXPERIENCING A LOT OF EXACERBATIONS OF CHRONIC CONDITIONS AND THEY ARE ALSO GENERATING HIGH COSTS FOR OUR HEALTH CARE SYSTEM.
SO THROUGHOUT THE HEALTH CARE WORLD HA HEALTH SYSTEMS HAVE INVESTED IN WHAT IS CALLED HIGH RISK HEALTH CARE SYSTEMS, A RESOURCE THAT'S SCARCE AND THAT HEALTH SYSTEMS HAVE TO DISTRIBUTE TO PEOPLE WHO NEED IT MOST.
THAT'S LIKE YOU KNOW HOME VISITS AND PRIMARY CARE SLOTS AND A LOT OF EXTRA HELP THAT IT SELF-COSTS MONEY.
SO WE'RE TRYING TO FIND PEOPLE TO HELP SO WE CAN PREVENT THEIR HEALTH CARE PROBLEMS SO WE CAN SAVE THE HEALTH CARE SYSTEM MONEY, BUT THAT'S A SCARCE

RESOURCE ON ITS OWN.
WE NEED TO TARGET THAT TO THE PEOPLE WHO NEED IT MOST SO THAT'S HOW ALGORITHMS COME IN.
SURPRISED ME WHEN I FIRST LEARNED ABOUT IT, WE STUDIED A PARTICULAR SET OF SOFTWARE THAT ITSELF WOULD USED TO SCREEN ABOUT 70 MILLION PEOPLE A YEAR AT HEALTH CARE SYSTEMS THROUGHOUT THE U.S.
IF YOU LOOK AT THE FAMILY OF ALGORITHMS THAT WORK JUST LIKE THE ONES WE STUDIED, THOSE ARE USED FOR 10050 TO 200 MILLION PEOPLE A YEAR, THE MAJORITY OF THE U.S. POPULATION.
WHEN WE THINK OF THE THE SCALE OF ALGORITHMS, THAT'S WHERE THEY'VE STARTED OIMPACTING LIVES ON A VERY, VERY LARGE SCALE.
THESE ALGORITHMS ARE FINDING PEOPLE WHO ARE GOING TO GET SICK AND THE WAY THEY DO THAT IS THEY PREDICT.
ALGORITHMS ARE VERY GOOD AT LOOKING INTO THE FUTURE.
JUST LIKE ALGORITHMS ARE GOING TO FIGURE OUT WHAT PRODUCTS YOU'RE GOING TO BUY, WHAT MOVIES YOU'RE GOING TO LIKE, THESE LOOK AT HOW MUCH THIS IS GOING TO COST THE SYSTEM AND THEY MAKE THAT FORECAST AND THEY FIGURES OUT OKAY THIS PERSON LOOKS LIKE SHE'S GOING TO COST A LOT OF MONEY WITH ALL THESE E PRMPLET VISITS AND HEALTH CARE SHE'S GOING TO SCHOOL, LET'S TARGET HER WITH EXTRA HEM.
NOW GIVEN HOW WIDELY USED THESE ALGORITHMS ARE, WE WERE REALLY INTERESTED IN THE QUESTION OF WHETHER OR NOT THEY WERE

RACIALLY BIASED.
NOW TO STUDY RACIAL BIAS IN AN ALGORITHM, YOU NEED TO STUDY EXACTLY WHAT YOU MEAN BY BIAS.
HERE IS HOW WE DIT.
WE TARGETED A PRINCIPLE OF -- WE ARTICULATED, CRAWMS THROUGH A POPULATION OF PATIENTS.
SO IF YOU ARE WORKING AT A HOSPITAL OR AN INSURER, YOU HAVE A POPULATION OF PATIENTS YOU'RE RESPONSIBLE FOR.
AND ONCE OR TWICE A YEAR THAT ALGORITHM IS GOING TO GENERATE A SCORE AND THAT SCORE IS GOING DO PRIORITIZE IF YOU GET HELP OR SCREENED OUT.
PEOPLE WHO GET THE SAME SCORE ARE GOING TO BE TREATED THE SAME BAY.
AS A RESULT, THOSE PEOPLE SHOULD HAVE THE SAME NEEDS, IN TERMS OF THE NEED FOR EXTRA HELP AND THE COLOR OF THEIR SKIN DEFINITELY SHOULDN'T MATTER.
BUT THAT'S NOT WHAT WE FOUND.
I'M GOING TO SHOW YOU A GRAPH AND WALK THROUGH THE AXIS VERY CAREFULLY, BECAUSE THIS TENDS TO BE A GENERAL CONCEPT.
WE'VE RANKED PATIENTS FROM LOW TO HIGH RISK.
THE TOP TWO OR 3%, ALL DID WAY ON THE PURPLE SIDE OF THAT GRAPH AND THE LAST LITTLE BIT ON THE RIGHT THOSE ARE THE PEOPLE THAT ARE GOING TO GET FAST TRACKED INTO THIS EXTRA HELP PROGRAM.
THE X CAN EXIST IS WHAT THE ALGORITHM THINKS IS GOING DO HAPPEN, IN THE Y A IS I'M SHOWING YOU WHAT REALLY HAPPENED.
THIS IS HOW MANY CHRONIC

CONDITIONS DO YOU HAVE, THAT FLARE UP OVER THE COURSE OF THAT NEXT YEAR?
AND CAN YOU SEE THERE ARE TWO LINES THERE.
THE TOP LINE PURPLE LINE IS BLACK PATIENTS AND THE YELLOW LINE IS WHITE PATIENCE.
NO MATTER WHERE WE ARE ON THAT GRAPH THE BLACK PATIENTS' LINE IS ABOVE WHERE THE WHITE BEING PEOPLE'S LINE IS.
NO MATTER WHERE YOU LOOK BLACK PATIENTS GO ON TO HAVE WORSE HEALTH THAN WHITE PATIENTS EVEN THOUGH THEY'RE TREATED THE SAME AND THEY HAVE THE SAME PRIORITY FOR GETTING EXTRA HELP.
HOW MUCH BIAS ARE WE TALKING ABOUT HERE?
IT IS A LITTLE HARD TO TELL FROM THE GRAPH SO LET'S GIVE YOU NUMBERS.
WHEN WE LOOKED AT THE PROGRAM THAT PEOPLE GET PRIORITIZED BY THE ALGORITHM, IT IS 18% BLACK TODAY.
CAN YOU LOOK AT THAT AND THINK OKAY, WHAT'S THE POPULATION RATE OF BLACK PATIENTS THAT THIS HIGH PRIORITY GROUP IS DRAWN FROM?
AND THAT'S ACTUALLY ONLY 12% BLACK.
SO AT FIRST GLANCE YOU MIGHT LOOK AT THAT AND SAY OH, BLACK PATIENTS ARE 50% OVERREPRESENT INSTEAD THAT GROUP.
THE ALGORITHM CAN'T BE BIASED.
IT IS OVERREPRESENTING BLACK PEOPLE IN THIS GROUP.
WHEN WE DID A SIMULATION THOUGH TO FIGURE OUT WHAT THAT GROUP SHOULD HAVE LOOKED LIKE, WHAT PROPORTION OF BLACK PATIENTS

SHOULD HAVE BEEN IN THAT HIGH
PRIORITY GROUP IT
DEVELOPMENTALLY SHOULD HAVE BEEN
47% BLACK.
SO IT'S AN ENORMOUS AMOUNT OF
BIAS THAT REDUCED THE FRACTION
OF BLACK PATIENTS IN THAT
PROGRAM FROM 14% TO 18%.
SO IN THE NEXT GRAPH I'M GOING
TO SHOW YOU ANOTHER GRAPH AND
THIS GRAPH SHOWS YOU AN
IMPORTANT ASPECT OF WHY THE
ALGORITHM IS GOING WRONG.
WE WANTED TO SHOW HOW THAT BIAS
GOT IN AND ONE KEY TO THAT IS
WHERE THE ALGORITHM WAS GOING
RIGHT.
ON THIS GRAPH ON THE X AXIS, I'M
SHOWING WHAT HAPPENS TO THEIR
COSTS AND CAN YOU SEE THAT THOSE
TWO LINES ARE RIGHT ON TOP OF
EACH OTHER.
SO WHEN THE ALGORITHM PREDICTS A
CERTAIN SCORE, THOSE PEOPLE GO
ON TO HAVE THE SAME COSTS.
SO THE ALGORITHM IS PREDICTING
TOTAL HEALTH CARE HE COSTS VERY
ACCURATELY WITHOUT MUCH
DIFFERENCE BETWEEN BLACK AND
WHITE PATIENTS.
LET ME SHOW YOU THE ALGORITHM IS
BIASED FOR PREDICT RG HEALTH BUT
UNBIASED PREDICTING COST.
THAT'S BECAUSE BLACK AND WHITE
PATIENTS DON'T HAVE THE SAME
RICH BETWEEN COST, WHITE
PATIENTS HAVE BETTER ACCESS TO
THE HEALTH CARE SYSTEM.
THEY'RE NOT GOING TO STAY AT
HOME, THEY'RE GOING TO SEE A
DOCTOR THEY'RE GOING TO GENERATE
MORE COSTS EVENING WHEN THEY
HAVE THE SAME NEEDS.
WHEN YOU HAVE A SQUEEZING

SENSATION IN YOUR CHEST AND
SITTING ON YOUR COUCH YOU'RE
MONTH MORE LIKELY TO CALL THE
AMBULANCE AND GET TESTED, IF YOU
ARE WHITE THAN YOU'RE BLACK.
THERE'S LOTS OF EVIDENCE OF
SYSTEMIC RACISM AND HOW DOCTORS
DEVELOPMENTALLY RECOMMEND TESTS
AND TREATMENTS FOR BLACK
PATIENTS.
SO THE RESULTS OF ALL OF THIS IS
CONDITIONAL ON SOMEONE'S HEALTH,
TWO PEOPLE ARE GOING TO HAVE
DIFFERENT COSTS VERSUS BLACK
VERSUS WHITE.
COSTS MEANS BIAS WHU ARE
PREDICTING HEALTH.
LET ME TRY TO DISTILL SOME
LESSONS FROM THAT STUDY BEFORE
STEPPING BACK AND TEASING OUT
THE IMPLICATIONS.
A REALLY IMPORTANT PART OF WHAT
WE DID IS ARTICULATE THAT IDEAL
ALGORITHM.
THE ALGORITHM IS BEING USED TO
DECIDE WHO GETS WHAT IN TERMS OF
EXTRA HELP FOR SOMEONE'S HEALTH
SO THOSE PEOPLE AT A GIVEN
ALGORITHM SCORE, THE ALGORITHM
SHOULD BE PREDICTING HEALTH AND
THOSE PEOPLE SHOULD HAVE THE
SAME HEALTH NEEDS.
THAT'S HOW YOU HOLD AN ALGORITHM
ACCOUNTABLE BY ARTICULATING WHAT
THE TARGET IS THAT IT'S SUPPOSED
TO BE PREDICTING, IN THIS CASE
HEALTH AND COMPARING IT IN THIS
CASE TO WHAT IT'S ACTUALLY
INDICATING AND THAT'S COST.
EVEN THOUGH IT'S SUBTLE THIS IS
IS SOURCE OF A LOT OF GRIMPLIC
BIAS IN THE SYSTEM.
WE HAVE A ROAD PLAN FOR FIXING
IT.

ONCE WE ARTICULATED THIS PROBLEM
WE REALIZED THE ALGORITHM WAS
PREDICTING THE WRONG HAVE A
VARIABLE.
WE WERE ABLE TO RETRAIN TO IT
PREDICT HEALTH RATHER THAN COST.
THAT REALLY HELPED AND IT
REDUCED THE BIAS IN THAT
ALGORITHM BY ONE MEASURE BY 84%.
THAT LESSON, WE HAVE TO
ARTICULATE THE ALGORITHM, MAKE
SURE THE ALGORITHM IS DWHIENG
IT'S SUPPOSED TO DO IS A THEME
THAT'S COME UP AGAIN AND AGAIN
OVER THE PAST TWO YEARS AS WE'VE
WORKED WITH A LOT OF HEALTH CARE
SYSTEMS, INSURERS, DEC
COMPANIES, AT THE STATE AND
FEDERAL LEVEL.
I WANT TO GIVE YOU A SENSE OF
THAT WORK IS DHOO WE'VE FOUND
THIS SAME BIAS, THE
DISCREPANCIES BETWEEN WHAT THE
ALGORITHM IS IDEALLY SUPPOSED TO
BE DOING AND WHAT IT'S ACTUALLY
DOING IS WIDESPREAD AMONG HEALTH
CARE SYSTEM.
HEALTH CARE NEEDS VERSUS TOTAL
COSTS.
WHEN WE LOOK AT A NUMBER OF
THINGS FOR EXAMPLE ON THE SECOND
TO LAST ROW, A LOT OF THE HEALTH
CARE SYSTEMS ARE USINGS,
ALGORITHMS, IS A PERSON GOING TO
SHOW UP FOR AN APPOINTMENT?
IF THAT ALGORITHM PREDICTS
YOU'RE NOT GOING TO SHOW UP,
IT'S GOING TO TAKE IT AWAY FROM
YOU AND REASSIGN TO IT ANOTHER
PATIENT.
OF COURSE PEOPLE CANNOT SHOW UP
TO THE DOCTOR FOR A COUPLE OF
REASONS.
ONE THING, THEY REALIZE THEY

DIDN'T NEED HEALTH CARE AT ALL.
BUT SOME PEOPLE DON'T SHOW UP
BECAUSE THEY FACE BARRIERS TO
ACCESSING CARE.
THEY'RE MORE LIKELY TO BE BLACK
AROUND MORE LIKELY TO BE POOR,
THE LAST THING YOU WANT TO DO IS
REASSIGN THAT SLOT TO ANOTHER
PATIENT.
YOU DON'T WANT TO REBOOK THEIR
SLOT TO SOMEONE WHO NEEDS IT
LESS.
SO THESE KINDS OF BIASES ARE
ACTIVE THROUGHOUT THE HEALTH
CARE SYSTEM.
DID YOU THINK BIT THEY'RE ALSO
VERY ACTIVE IN A LOT OF OTHER
INDUSTRIES.
SO IN CRIMINAL JUSTICE, A LOT OF
ALGORITHMS ARE TRYING TO PREDICT
SOMEONE'S INNATE TENDENCY TO
COMMIT A CRIME BUT WE DON'T SEE
THEIR INNATE TENDENCY TO COMMIT
A CRIME, WE SEE WHETHER OR NOT
THEY GET ARRESTED, GET
CONVICTED, AND THOSE TWO ARE NOT
THE SAME ESPECIALLY IF YOU LOOK
AT THOSE THROUGH THE LENS OF
RATION.
IN FINANCE, WE ARE INTERESTED IN
PREDICTING CREDIT WORTHINESS.
WE PREDICT INCOME AND THAT IS
NOT THE SAME, ESPECIALLY SEEN
THROUGH THE LENS OF GENDER RACE
OR SOCIOECONOMICS.
IT IS WHEN WE ARE REGHTING A
DRUG WE UNDERSTAND THAT A DRUG
SHOULD DO MORE GOOD THAN HARM
AND EVEN IF WE CAN DISAGREE
ABOUT HOW MUCH GOOD OR HOW MUCH
HARM THAT IS THE STANDARD THAT
WE HOLD DRUGS TO.
WHEN WE'RE REGULATING A DOASER
OR OTHER APPLIANCE THE STANDARD

IS IT SHOULDN'T CATCH ON FIRE.
BUT WHAT ABOUT ALGORITHMS, WHAT VOCABULARY DO WE USE FOR REGULATING THEM?
WHAT I WOULD SUBMIT TO YOU IS THE GOAL POST THE TARGET WE WANT TO HOLD ALGORITHMS ACCOUNTABLE TO IS THAT IDEAL TARGET, THE ALGORITHM SHOULD BE PREDICTING.
IS THE ALGORITHM DOING WHAT IT'S SUPPOSED TO DO AND IS IT DOING EQUALLY WELL FOR BLACK AND WHITE PATIENTS?
THAT'S T
GROUP AND THE INTUITION THAT YIELDS A CRISP TEST, THE ALGORITHM'S ABILITY TO PREDICT THE OUTCOME DIFFERENT FOR WHITE OR BLACK PATIENTS?
WE HAVE A CLEAR PARALLEL TO CIVIL RIGHTS LAW AND THE USE OF PROXY VARIABLES WHICH CAN BE DISCRIMINATORY.
I WANT DO CLOSE BY TAKING SOME CONCRETE LESSONS ABOUT WHAT YOUR ORGANIZATION CAN DO TO MITIGATE ALGORITHMIC BIAS.
AS I MENTIONED OVER THE PAST COUPLE OF YEARS WE'VE BEEN WORKING WITH A LOT OF ORGANIZATIONS IN HEALTH BUT INCREASING REPLY OUTSIDE OF HEALTH IN FINANCE AND OTHER SECTORS AS WELL AND HERE ARE SOME FOUR STEPS THAT WE FOUND CAN BE TAKEN WITHIN ORGANIZATIONS THAT CAN REALLY HELP WHEN DEALING WITH ALGORITHMIC BIAS.
THE FIRST STEP IS TO DESIGNATE SOMEONE IN THE ORGANIZATION DHAS RESPONSIBLE FOR OVERSIGHT OF ALGORITHMS.
AND IMPORTANTLY, THAT PERSON

NEEDS TO BE AT A HIGH LEVEL.
VERY OFTEN DECISIONS ABOUT ALGORITHMS ARE PUSHED DOWN TO TECHNICAL STAFF AND ORGANIZATIONS WHO ARE EMPOWERED TO MAKE THESE HIGH LEVEL STRATEGIC DECISIONS OR TO ENGAGE.
>> OVERSIGHT ACTIVITIES ABOUT HOW ALGORITHMS ARE BEING USED.
SO MUCH LIKE IN OTHER PARTS OF REGULATION AND LAW, WE NEED SOMEONE AT A HIGH LEVEL IN AN ORGANIZATION WHO IS ULTIMATELY RESPONSIBLE FOR OVERSIGHT AND THAT PERSON NEEDS TO BE ADVISED BY, EMABOUT POWERED TO RAISE ISSUES AND ASK QUESTIONS.
NUMBER TWO, ONE THING WE FOUND IS THAT MOST ORGANIZATIONS ACTUALLY DON'T KNOW WHAT ALGORITHMS ARE BEING USED INSIDE OF THEIR OWN-OS.
AND I THINK THAT'S REALLY SURPRISING BECAUSE LET'S SAY YOU WERE AN EXECUTIVE WHO HADN'T CLI HYPOTHETICALLY DIDN'T KNOW, ANYONE CAN START ASKING QUESTIONS ABOUT WHAT ALGORITHMS ARE DOING AND HOW THEY ARE PERFORMING FOR THAT TASK.
NUMBER 3 ALGORITHMIC PERFORMANCE NEEDS TO BE DOCUMENTED.
INTERESTINGLY WHEN WE ASK ABOUT AN ALGORITHM, WHEN IT COMES TO HELPING A HEALTH CARE SYSTEM DO BETTER, ORGANIZATIONS AND THE STAFF THAT ARE AT THOSE ORGANIZATIONS HAVE NO IDEA WHERE THE ALGORITHM CAME FROM, WHAT IT DOES, HOW IT'S PERFORMING, THEY OFTEN SAY BOB MADE THAT, BOB LEFT A COUPLE OF YEARS AGO BUT WE'RE STILL USING THAT

ALGORITHM.
THAT'S A DANGEROUS SITUATION TO BE IN BOTH FOR STRATEGIC PURPOSES AROUND FOR BIAS PURPOSES.
FINALLY, WHEN ALGORITHMS ARE FOUND TO BE BIASED THEY NEED TO BE FIXED OR DELETED.
LET'S ARTICULATE SOME USE CASES FOR THESE LESSONS.
I THINK IF YOU ARE A STRATEGIC LEADER AT A HIGH LEVEL IN THE-O YOU NEED TO KNOW WHICH ALGORITHMS ARE OPERATING AT SCALE IN YOUR OPERATION AND YOU NEED TO THINK STRATEGICALLY HOW THOSE ARE BEING USED WHERE THEY CAN GO WRONG AND WHAT FIXES CAN YOU PUT IN PLACE.
YOU NEED TO BE ABLE TO RECOGNIZE AND WEIR THE SUBTLE TECHNICAL CHOICES THAT WE'VE FOUND CAN LEAD TO BIAS AND IF YOU ARE BUYING ALGORITHMS YOU NEED TO BE AN EDUCATED CONSUMER OF THOSE ALGORITHMS YOU ARE BUYING.
IF YOU ARE REGULATING ALGORITHMS YOU NEED TO HAVE CLEAR STANDARDS FOR WHAT ALGORITHMIC BIAS LOOKS LIKE BOTH SO YOU CAN CONDUCT INVESTIGATIONS AND CAN YOU PROVIDE GUIDANCE TO INDUSTRY ON HOW TO STAY ON THE RIGHT SIDE OF THE LAW.
THE LAST THING I'LL MENTION IS WE TRIED TO DISTILL THESE INTO A PLAY BOOK.
THE LINK TO THE PLAY BOOK SHOULD BE IN THE ACCOMPANYING MATERIAL IN THE PRIVACY CONWEBSITE.
YOU'LL FIND A LOT MORE DETAIL AND SOME SUMMARY STEPS ABOUT HOW TO APPLY THESE LESSONS.
WE'RE ALSO WORKING DIRECTLY WITH

ORGANIZATIONS TO HELP THEM
IMPLEMENT SOME OF THESE
PRINCIPLES WHEN THEY DON'T HAVE
THE INTERNAL CAPACITY SO I'D
URGE TO YOU REACH IDENTITY TO US
IF YOU ARE INTERESTED IN BEING
PART OF THIS WORK AND THANK YOU
VERY MUCH.
>> SO THANK YOU VERY MUCH ZIAD
FOR THIS PRESENTATION.
WE'VE TALKED ABOUT THIS A LOT,
THE CHALLENGE IS TO PICK WHERE
TO START.
LET ME START WITH THE QUESTION
ABOUT THE DATA YOU PRESENTED.
YOU SHOWED BASICALLY WHAT WAS AN
ESTIMATE TO SOME DEGREE OF THE
AMOUNT OF BIAS IN THE ALGORITHMS
THAT YOU WERE EVALUATING.
ONE QUESTION I HAVE IS ARE THERE
THRESHOLD FOR ACCEPTABLE LEVEL
OF BIAS?
I'M THINKING OF THAT IN TERMS OF
YOU CAN DETECT IMIEF, AN-O CAN
DETECT BIAS IN AN ALGORITHM AND
IMMEDIATELY BE FACED WITH THE
DECISION OF WHETHER OR NOT TO
CONTINUE TO USE THAT ALGORITHM
AND POTENTIALLY OR DISCONTINUE
USING THAT ALGORITHM AND
POTENTIALLY RISK GETTING ANY OF
THE INTFTS FROM ITS USE OR TRY
TO USE IT IN SOME LIMITED
CAPACITY.
THE QUESTION I HAVE IS HOW DO
ORGANIZATIONS SORT OF MAKE THAT
DETERMINATION WHEN BIAS IS
DETECTED?
>> YOU KNOW I THINK THERE ARE
TWO'S TO THIS QUESTION.
I THINK THERE'S A SIMPLE ANSWER
WHICH IS THAT I THINK IN MANY
LEGAL SETTINGS, THE STANDARD
THAT LOTS OF OTHER THINGS NOT

ALGORITHMS BUT ANY KIND OF
DISCRIMINATORY, POTENTIALLY
DISCRIMINATORY POLICY IS HELD TO
IS A VERY BASIC STATISTICAL
SENSE OF FAIRNESS.
IN OUR SETTING, LET'S TAKE THE
GROUP OF PEOPLE WITH THE SAME
ALGORITHM SCORE.
LET'S SEPARATOR THEM INTO THE
BLACK AND WHITE SUBPOPULATION,
LET'S STATISTICALLY CONSIDER,
WHAT HAPPENS TO PEOPLE, ON THE
IDEAL TARGET, AND TEST IF THOSE
GROUPS EVER STATISTICALLY
DIFFERENT.
THAT IS A STANDARD THAT HAS BEEN
HELD TO OTHER INSTANCES OF
DISCRIMINATION.
SO THAT'S KIND OF A STATISTICAL
ANSWER.
THERE IS A DEEPER QUESTION THAT
YOU ARE ASKING I THINK SO LET ME
DISTINGUISH FROM TWO SETTINGS.
IN HEALTH, IN THIS SETTING THAT
WE TALKED ABOUT YEAR TRYING TO
FIND PEOPLE WHO NEED EXTRA HELP
AND TARGET RESOURCES TO THE
PEOPLE WHO NEED EXTRA HELP.
IN THAT SETTING IT'S A REAM
PROBLEM BOTH IN TERMS OF BIAS
BUT IN TERMS OF JUST WHAT THE
ALGORITHM IS SUPPOSED TO BE
DOING.
IF THAT EXTRA HELP ISN'T GOING
TO THE RIGHT PEOPLE.
WHAT WE FOUND IS THAT IT WASN'T
GOING TO THE RIGHT PEOPLE AND
THE PEOPLE THAT WERE MISSING OUT
WERE MORE LIKELY TO BE BLACK.
SO THERE'S BOTH A GREAT BUSINESS
CASE FOR FIXING THE ALGORITHM
AND A GREAT CASE FOR ANYONE WHO
IS INTERESTED IN PROMOTING
RACIAL EQUITY.

THAT'S OFTEN THE CASE IN HEALTH,
WE WANT THE RESOURCE TO GO TO
THE PEOPLE WHO NEED IT AND THOSE
PEOPLE ARE OFTEN MORE
DISADVANTAGED.
IN OTHER SETTINGS, IN FINANCE
FOR INSTANCE, THE STRUCTURE IS A
LITTLE BIT DIFFERENT.
IN CASE OF HISTORICAL
DISCRIMINATION, PEOPLE WHO NEED
CREDIT ARE OFTEN LESS LIKELY TO
REPAY LOANS.
SO IN THAT SETTING THERE IS A
LEGAL STANDARD AROUND BUSINESS
NECESSITY WHICH DO STAY AFLOAT
CREDITORS CAN'T BE GIVING LOANS
TO PEOPLE WHO WON'T REPAY.
FINDING PEOPLE WHO ARE GOING TO
PAY BACK LOANS AND PRICING THE
CREDIT ACCORDINGLY.
SO I THINK THAT THAT'S MAYBE THE
OTHER PART OF THE LEGAL STANDARD
IS THAT WE DO HAVE LAWS THAT
PROVIDE FOR THIS BUSINESS
NECESSITY PURPOSE FOR ALGORITHMS
AND THAT IS THE CATEGORY THAT I
WOULD PUT IT IN.
SO IS IS IT A QUOTE UNQUOTE
ACCEPTABLE LEVEL OF BIAS?
IT'S NEVER A ACCEPTABLE LEVEL OF
BIAS BUT UNDER LAW, THERE IS A
BUSINESS NECESSITY, FOR PEOPLE
TO BE CHARGED A HIGHER RATE TO
ACCURATELY REPRESENT THAT RISK
OF NOT PAYING BACK A LOAN.
AT LEAST IN OUR WORK WITH
REGULATORS IS APPLIED TO
ALGORITHMS AS WELL.
>> MOVING TO YOUR WORK DIRECTLY
WITH ORGANIZATIONS, CAN YOU TALK -- SORRY ABOUT THAT.
CAN YOU TALK A LITTLE BIT ABOUT
THE COST ASSOCIATED WITH
APPLYING THE PLAY BOOK?
SO YOU GIVE A LOT OF PRACTICAL

TICHES ABOUT THAT ORGANIZATIONS
CAN ACTUALLY USE BUT IN YOUR
EXPERIENCE, CAN YOU DISCUSS THE
COSTS THAT ARE INCURRED SO LIKE
WERE THERE SIGNIFICANT COSTS IN
HIRING STAFF IN ORDER TO AUDIT
ALGORITHMS, ARE THERE
SIGNIFICANTLY ADDITIONAL COST
$INCURRED BY ORGANIZATIONS?
>> SO THE WAY WE TRIED THE
STRUCTURE THE PLAY BOOK WAS
REALLY GROUNDED IN THE WORK THAT
WE'VE BEEN DOING WITH
ORGANIZATIONS OVER THE PAST
COUPLE OF YEARS AND THAT WORK
WAS USING EXISTING RESOURCES.
SO USING THE TECHNICAL TEAMS
THAT ARE ALREADY DEPLOYED WITHIN
AN ORGANIZATION.
AND APPLYING SOME OF THESE
PRINCIPLES FROM THE PLAY BOOK WE
WERE ABLE TO CONDUCT AN
INVENTORY OF ALGORITHMS,
IDENTIFY POTENTIALLY PROBLEMATIC
ONES AND AUDIT THEM WITHOUT
HIRING NEW STAFF, WITHOUT
DEVOTED OING ADDITIONAL
RESOURCES TO IT.
HOW INTENSIVE IS IT TO EXISTING
RESOURCES?
YOU NEED TO ALLOCATE TIME IN
ACTUALLY BUILDING UP THAT
INVENTORY.
PUTTING TOGETHER A LOT OF
INFORMATION FROM DIFFERENT
BUSINESS UNITS IN THE
ORGANIZATION.
YOU ALSO NEED TO BE VERY
THOUGHTFUL ABOUT ARTICULATING,
OKAY WHAT IS THIS ALGORITHM
SUPPOSEDLY TO BE DOING?
WHAT IS IT ACTUALLY DOING?
IS THAT A SUBSTANTIAL COST, I
THINK ITS REQUIRES LIKE PART OF

AN FTE FOR A FEW MONTHS TO DO
THIS REALISTICALLY AND THAT'S
WHAT WE'VE SEEN IN ORGANIZATIONS
BUT WOULD I SAY THAT IT'S ALMOST
AN ILLUSION DO THINK THAT
THERE'S NO COST TO LETTING THE
STATUS QUO BE THE STATUS YOA.
QUO.
WHAT WE'VE SEEN OVER AND OVER
AGAIN IN A LOT OF ORGANIZATIONS
IS THERE ARE FUNDAMENTALLY
FLAWED ALGORITHMS THAT ARE
AFFECTING THOUSANDS IN SOME
CASES MILLIONS OF CUSTOMERS OF
PATIENTS AT SCALE.
SO THERE'S A HUGE COST BOTH IN
TERMS OF REGULATORY RISK AND
JUST IN TERMS OF ALGORITHMS NOT
FIT FOR BUSINESS PURPOSE IN NOT
DOING THESE THINGS.
AND SO I THINK THAT'S WHY I
THINK IT'S AN ILLUSION TO TRY TO
SAVE COSTS BY NOT DOING THESE
THINGS.
THESE THINGS ARE EVENTUALLY
GOING TO COME TO LIGHT WHETHER
IT'S IN BAD BUSINESS DECISIONS
OR IN TERMS OF REGULATORY
EXPOSURE.
SO I THINK THIS IS A PRETTY GOOD
INVESTMENT OF A SMALL AMOUNT OF
RESOURCES CONSIDERED ON AN
ORGANIZATIONAL BASIS.
>> THAT REALLY RECESS
NECESSITATES REQUEST ME BECAUSE
FROM A SECURITY ADAPT, WE MAKE
THE SAME, UP FRONT COSTS TEND TO
BE BETTER THAN THE COSTS YOU
TEND TO PAY ON THE BACK END
AFTER AN INCIDENT OCCURS.
THAT MAKES TOTAL SENSE.
>> THAT ARGUMENT SOMETIMES
AREN'T AS PERSUASIVE TO PEOPLE.
>> MAYBE SOME FTC FINES HAVE

HELPED WITH THAT.
DO YOU HAVE RECOMMENDATIONS FOR INFORMATION THAT ORGANIZATIONS CAN PROVIDE TO SHOW THAT THEIR ALGORITHMS HAVE BEEN SUBJECTED TO A REASONABLE PROCESS OR HAVE BEEN AUDITED IN SOME MEANINGFUL WAY?
I GUESS CONFERSLY QUESTIONS THAT CONSUMERS CAN ASK TO TRY TO UNDERSTAND THAT THE ALGORITHMS THAT THEY ARE BEING SUBJECT TO HAVE ACTUALLY BEEN VETTED IN SOME WAY TO TRY TO IDENTIFY BIAS?
>> IT'S A REALLY GREAT QUESTION BECAUSE I THINK YOU KNOW UNLIKE IN A LOT OF OTHER INDUSTRIES, IN FINANCE THERE IS ENORMOUS DOCUMENTATION REQUIREMENTS DOLLAR IMPOSED ON COMPANIES BY THE REGULATORY SYSTEM.
AND I THINK IN THESE ALGORITHMIC TETINGS THERE IS NO CORRESPONDING NEED TO DOCUMENT WHAT THE ALGORITHM IS DOING OR HOW IT'S PERFORMING OR THAT IT'S UNBIASED.
LET ME KIND OF 50 YOU TWO THOUGHTS BASED ON OUR WORK THAT WENT INTO THE PLAY BOOK.
NUMBER ONE IS THAT THE INVENTORY AND IF DOCUMENTATION OF PERFORMANCE OF AN ALGORITHM ACTUALLY DOESN'T NEED TO BE PUBLIC.
IT SHOULD BE MAINTAINED INTERNALLY AND IT SHOULD BE KEPT ON FILE SO THAT DID ANYONE ASKS -- IF ANYONE ASKS QUESTIONS THAT INFORMATION IS AVAILABLE AND A COMPANY CAN VERY EASILY SHOW THAT THE ALGORITHMS THAT IT'S USING ARE BOTH DOING WHAT

THEY'RE SUPPOSED TO BE DOING AND NOT INTRODUCING BIAS INTO THE DECISIONS.
ON THE OTHER HAND, I THINK THAT YOU KNOW ALL OF THE WORK THAT WE'VE DONE DOESN'T REQUIRE OPENING UP THE BLACK BOX OF THE ALGORITHM AND SO IN ORDER TO DO THE WORK THAT WE PUBLISHED IN OUR ORIGINAL PAPER A COUPLE OF YEARS AGO OR ANY OF THIS WORK THAT WE'VE DONE IN THE PLAY BOOK WHAT WE NEED ARE THE ALGORITHM SCORES AND SOME READOUT OF WHAT THE IDEAL TARGET WOULD BE.
SO IN THIS SETTING THIS WAS HOW DID THE PATIENT DO IN TERMS OF THEIR HEALTH?
PUTTING THOSE DATA TOGETHER IS ACTUALLY SOMETHING THAT DOESN'T NEED TO COMPROMISE TRADE SECRETS.
IT CAN BE DONE BY AN EXTERNAL AUDITOR VERY EASILY WITH THE RIGHT DATA.
AND SO I THINK THAT THOSE KINDS OF AUDITS ARE APPEALING BECAUSE THEY DON'T REQUIRE US TO DO A LOT OF COMPLEX WORK ON THE INSIDE OF THE ALGORITHM OR OPEN UP THE BOX OR YOU KNOW TO THE PREVIOUS SESSION'S POINT THERE ARE LOTS OF TRANSPARENCY METHODS FOR ILLUSTRATING EXACTLY WHAT THE ALGORITHM IS DOING.
OUR METHOD ACTUALLY DOESN'T REQUIRE THAT.
WE JUST NEED THE SCORE AND THIN THE ULTIMATE JUDGE OF WHETHER THE ALGORITHM IS DOING WHAT IT'S SUPPOSED DO DID IN THE FORM OF AN IDEAL TARGET.
>> I THINK THAT'S REALLY A GREAT POINT THAT THE POINTS OF NOT

OPENING UP THE BLACK BOX.
SOME ORGANIZATION HE FEEL RELUCTANT TO SHARE, IT'S NICE TO KNOW THAT COMPANIES CAN GO THROUGH THIS PROCESS AND SHARE INFORMATION ABOUT THE LACK OF BIAS IN THEIR -- IN THEIR ALGORITHMS WITHOUT REVEALING TRADE SECRETS.
I THINK RELATED TO THAT POINT AND ALSO MENTIONING SOMETHING FROM THE PREVIOUS PANEL, I'M WONDERING, THE DEGREE TO WHICH THAT'S TRUE IN THE FACE OF USING PROXY VARIABLES.
THE PREVIOUS PANEL TALKED ABOUT PROXY VARIABLES FROM GENDER AND RACE, CAN YOU GET THAT SAME GUARANTEE OF BEING ABLE TO THOROUGHLY ANALYZE AN ALGORITHM AND WITHHOLD SORT OF THE PROPRIETARY INFORMATION IN THE FACE OF PROXY VARIABLES OR OTHER USE OF PROXY VARIABLES?
>> IN HERE LET ME JUST MAKE SURE I UNDERSTAND.
THESE ARE THE PROXY VARIABLES THAT YOU NEED TO WHEN YOU DON'T HAVE ACCESS TO SOMEONE'S SELF-REPORTED RACE?
THE ONES THAT CAN BE IMPUTED USING LIKE THE CONSUMER FINANCIAL PROTECTION BUREAU METHOD OR THINGS LIKE THAT ARE THOSE THE PROXIES YOU MEAN?
>> OR PROXIES THAT ARE DEFINED INTERNALLY BY THE ORGANIZATION ITSELF.
IF THEY'RE DIFFERENT CONTEXT MAYBE YOU CAN TALK ABOUT WHERE THE DIFFERENCE LIES.
>> IT IS COMMON FOR INSURERS NOT TO HAVE DATA ON THE RAISE PPED TONPEOPLE THEY ARE INSURING.

ONE SOLUTION IS YOU CAN OFTEN GET THOSE DATA DID THEY ARE IMPORTANT.
SO FOR EXAMPLE ONE HEALTH INSURER WE ARE WORKING WITH IS REQUESTING SELF REPORTED RACE INFORMATION ON THEIR INSURED POPULATION FROM THE HEALTH CARE SYSTEMS, THE HEALTH CARE SYSTEMS HAVE THOSE DATA BECAUSE THEY CAN ASK THE PATIENT DIRECTLY AND IF THE INSURER WANTS THAT THEY CAN MERGE THAT.
THERE ARE PLACES YOU CAN PURCHASE THAT DATA AND MERGE THAT IN, JUST LIKE YOU CAN PURCHASE SOMEONE'S CREDIT SCORE AND MERGE THAT IN.
I THINK THOSE TWO OPTIONS ARE BOTH SOMEWHAT UNDERRATED.
I THINK HISTORICALLY WE HAVEN'T PRIORITIZED GETTING THIS INFORMATION AND IT'S ALMOST LIKE SOMETIMES COMPANIES DON'T WANT TO KNOW BECAUSE DHEAR UNDER THE IMPRESSION THAT OH DID I DON'T KNOW ABOUT DISPARITIES I CAN'T BE HELD ACCOUNTABLE FOR THEM.
AND I THINK FROM MY INVOLVEMENT IN SOME CIVIL INVESTIGATIONS THAT I UNFORTUNATELY CAN'T TALK ABOUT I CAN ASSURE YOU THOSE ARE NOT THE CASE.
I DON'T THINK THOSE ARE THE CASE AT THE FEDERAL LEVEL EITHER.
I THINK THOSE ARE IMPORTANT DO FLAG.
OARPD, THE CONSUMER PROCESSING BUREAU HAS A METHOD OF IMPUTING SOMEONE'S RACE BASED ON A COMBINATION OF ZIP CODE AND OTHER DATA YOU HAVE.
IN CASES YOU DON'T HAVE THE REAL VARIABLE AND YOU HAVE TO RELY ON

PROXIES.
>> I ANY THAT'S GREAT AND I REALLY WANT TO SORT OF CONFIRM MY UNDERSTANDING OF WHAT YOU'RE SAYING WHICH IS THAT THE USE OF PROXIES SHOULDN'T NECESSARILY BE A LIMITED FACTOR IN AN ORGANIZATION'S ABILITY TO AUDIT THESE ALGORITHMS FOR BIAS.
>> YES I THINK THAT'S CORRECT.
>> OKAY.
>> CERTAINLY, THOSE BROISMS EVEN IF THEY'RE IMPERFECT ARE CERTAINLY GOING TO GIVE YOU A READOUT.
THEY ARE GOING TO BE COORDINATED WITH THE REAL VARIABLES WITH THE CAVEATS, IF THEY'RE NOT EXACTLY RIGHT.
FROM AN OPTICS POINT OF VIEW ONE THING I'VE FOUND IS REGULATORS WANT BIASED ALGORITHMS NOT TO BE USED.
AT LEAST THE ONES WE'VE BEEN WORKING WITH, THERE HASN'T BEEN A PUNITIVE OR REASONABLE STANDARD OF HEALTH, IF YOU ARE MAKING GOOD FAITH EFFORTS TO UNDERSTAND THE BIASES IN THE ALGORITHMS THAT GOES A LONG WAY AND THE PROXIES CAN IS HELP WITH THAT.
>> ZIAD WE CAN GO OVER THIS FOR HOURS.
I REALLY WANT TO THANK YOU AGAIN FOR TAKING THE TIME TO PRESENT TO THE PRIVACY CON COMMUNITY AND LET'S SEE NEXT UP WE HAVE A SHORT BREAK AND WE'LL RECONVENE WITH THE NEXT PANEL AT 10:55.
ZIAD THANK YOU FOR TALKING TO YOU.
>> THANK YOU SO MUCH FOR HAVING ME.

>> HELLO, AND WELCOME TO PANEL 2.PRIVACY CON 2021.
MY NAME IS DANIELLE ESTRADA AND I'M AN ATTORNEY AT THE FEDERAL TRADE COMMISSION.
I'D LIKE TO WELCOME TO YOU THIS PANEL ENTITLED PRIVACY CONSIDERATIONS, AN UNDERSTANDING.
WE LOOK AT ISSUES SUCH AS HOW DO WE ENSURE THAT USERS, PRIVACY CHOICE HES AND WHEN THEY'RE AFFECTED BY DATA BREACHES.
WHAT CAN WE LEARN FROM THEIR RESPONSES.
I'M JOINED BY A GROUP OF DWRISHED CAN SCHOLARS WHO WILL BE PRESENTING THEIR RESEARCH ADDRESSING DIFFERENT WAYS TO MEASURE AND UNDERSTANDING DATA BREACHES AS WELL AS DIFFERENT APPROACHES TO IMPROVE USER DECISION MAKING, AND INCREASE AWARENESS.
YOU WILL HEAR FROM NICO EBERT OF ZURICH UNIVERSITY OF APPLIED SCIENCES PRESENTING THE PAPER BOLDER IS BETTER, RAISING USER AWARENESS THROUGH SALIENT AND CONCISE PRIVACY NOTICES.
ING SIDDHANT ARORA, CARNG GEE MILL LON UNIVERSITY.
OPT OUT STATEMENTS FROM PRIVACY POLICY TEXT.
CAMERON KORMYLO A VIRGINIA TECH, PRESENTING HIS PAPER, RECONSIDERING PRIVACY CHOICES, THE IMPACT OF DEDPAWLTS, REVERSEIBILTY AND REPETITION AND FINALLY, PETER MAYER OF KARLSRUHLE CAN INSTITUTE OF TECHNOLOGY, PRESENTING NOW I'M A BIT ANGRY, INDIVIDUALS REACTIONS AND RESPONSES TO DATA BREACHES

THAT AFFECTED THEM.
AS OF BEFORE, PLEASE REMEMBER TO
SUBMIT YOUR QUESTIONS TO E-MAIL
VIA PRIVACY CON@FTC.GOV.
I WILL BE ASKING EACH OF THE
PRESENTERS QUESTIONS, AND OPEN
UP THE DISCUSSION AT THE ENDS,
DID WE HAVE TIME.
FINALLY, I ENCOURAGE YOU AFTER
THE PRESENTATION TO GO TO THE
PRIVACY CON 2021 PAGE AT FTC.GOV
TO ACCESS THEIR FULL PAPERS.
WITH THAT, I WOULD LIKE TO TURN
IT OVER TO NICO EBERT TO
PRESENTLY HIS RESEARCH.
>> THANK YOU VERY MUCH DANIELLE.
MYT5()i(PiìCEIEKbT
DANIELLE.
MY NAME NECO, EBERT FROM ZAHW.
I'LL BE TALKING ABOUT PRIVACY
NOTICES, PROBABLY ONE OF THE
MOST BORING TOPICS IN THE WORLD
I HOPE TO SHOW YOU IT DOESN'T
HAVE TO BE THIS BORING, WE HAVE
WORK WE CONDUCT TOGETHER AND ALL
PAPERS TITLED,BOLDER IS BETTER
RAISING USER AWARENESS THROUGH
SALIENT AND CONCISE PRIVACY
NOTICES.
NEXT SLIDE AND THE QUESTION IS
LIKE, IS IT POSSIBLE TO RAISE
PRIVACY AWARENESS WITH SHORT
PRIVACY STATEMENTS?
WE'VE ALL SEEN THESE KIND OF
LIKE SHORT NOTICES WE MIGHT NOT
LIKE ACTIVELY HAVE LOOKED AT
THEM BUT COMPANIES HAVE STARTED
TO USE THEM, FOR EXAMPLE, APPLE
AND APPLE PAY HAS THESE SMALL
NOTICES IN THEIR APS OR RECENTLY
WHAT'S UP AP USED SHORT TEXT
HINTS IN THEIR AP WHEN THEY
CHANGED THEIR GENERAL PRIVACY
TERMS AND CONDITIONS LET'S SAY

THEY TRIED TO CHANGE THE PRIVACY TERMS AND CONDITIONS.
AND THE QUESTION IS, DO THESE WORK IN ANY WAY?
DO CUSTOMERS PERCEIVE THESE KIND OF SHORT NOTICES IN ANY WAY OR DO PEOPLE JUST IGNORE THEM LIKE THEY IGNORE TRADITIONAL LONG LEGAL PRIVACY POLICY STATEMENTS THAT ARE LEGALLY REQUIRED?
SO IS THIS MORE EFFECTIVE THAN WHAT WE HAD BEFORE? THAT'S A QUESTION.
AND IN ORDER TO ANSWER THIS QUESTION, WE DID AN ONLINE EXPERIMENT.
NEXT SLIDE, LOCATED IN GERMANY, WE CREATED A INFECTIOUS FITNESS APPLICATION, WHICH LOOKED PRETTY WE'LL AND ASKED PARTICIPANTS IN AN EXPERIMENT TO GIVE US FEEDBACK TO THIS FITNESS TRACKING AP.
WHAT THE PARTICIPANT DIDN'T KNOW AT THE TIME WAS THAT WE PUT IN PRIVACY NOTICES LIKE VERY SHORT PRIVACY NOTICES IN DIFFERENT WAYS.
TO THE RIGHT YOU'LL SEE WHAT WAS INSIDE THESE NOTICES, WHICH TEXT WAS INSIDE THESE NOTICES AND THEY WERE IMBEDDED IN THESE APS.
WE HAD ABOUT 2,000 MORE THAN 2,000 PARTICIPANTS THAT USED OUR AP WITH THESE NOTICES DEPLOYED IN THE AP.
SO-AND-SO WE CHANGE DIFFERENT THINGS WITH REGARDS TO THESE PRIVACY NOTICE AND THE FIRST THING, AND THIS IS WHAT BRINGS US TO THE NEXT SLIDE WAS A LEVEL OF SALIENT CY, CHANGED IT IN THREE DIFFERENT WAYS, SHORT NOTICES WITH PRIVACY

INFORMATION, JUST HIDDEN BEHIND A LINK, STILL VERY COMMON AND PRACTICE.
THAT YOU HAVE TO CLICK A LINK IN ORDER TO GET TO THE PRIVACY INFORMATION.
WE CALL THIS POLICY VIA CLICK.
WE MADE AN EXCLUSIVE PRESENTATION, MEANING THAT EVERY USER WOULD HAVE TO SEE THE PRIVACY POLICY, SO BASICALLY, EVERYBODY SHOULD HAVE CHECKED THROUGH THE AP AND WOULD HAVE SEEN THE PRIVACY POLICY.
AND IN THE LAST DESIGN WE HAD USERS THAT SAW THEM PRIVACY INFORMATION JUST BELOW THE FEATURES, WE CALLED THIS IMBEDDED.
WHENEVER WE HAD A SPECIFIC FEATURE WE HAD TO RELATE A PRIVACY INFORMATION, NEXT TO THE FEATURE, WHICH IS VERY COMPARABLE THE WAY APPLE DID IT WITH APPLE PAY IN MY INTRODUCTION, THAT WAS ONE THING HOW SALIENT OUR PRIVACY INFORMATION WAS IMBEDDED IN THE AP AND THE SECOND NEXT WAS THE LEVEL OF RISK OF THE INFORMATION.
SO WHAT WE DID WAS WE HAD LIKE VERY PRIVATE FRIENDLY VERSION OF OR PRIVACY POLICY, AND WE HAD A VERY AGGRESSIVE PRIVACY INTRUSIVE VERSION OF OUR PRIVACY POLICY, ONE THAT PROBABLY NO COMPANY WILL EVER USE IF THEY ARE NOT FORCED TO DO SO, WHICH, FOR EXAMPLE, HAD STUFF IN IT WE, THIS AP RECORDS EVERYTHING YOU DO WITH YOUR MICROPHONE, THIS AP STORES YOUR LOCATION DATA FOREVER, THIS AP SAVES YOUR

LISTENING HABITS SONGS YOU
LISTEN WHILE RUNNING, AND IF
THEY ARE PIRATED IT'S DIRECTLY
REPORTED SO THIS WAS VERY
AGGRESSIVE TEXT BECAUSE THAT WAS
OUR ATTENTION OR I HYPOTHESES,
MAYBE NOBODY WILL EVER READ
THOSE TEXTS LET'S AT LEAST TRY
TO MAKE THEM VERY AGGRESSIVE,
PRIVACY INTRUSIVE.
TO SEE IF WE CAN ACTUALLY HAVE
SOME REACTION.
IN THE END WE ENDED UP WITH A
THREE BY TWO DESIGN MEANING THAT
WE HAD THESE MORE THAN TWO
STYLES OF PARTICIPANTS AND
ASSIGNED THEM TO DIFFERENT
GROUPS.
SO WE, ONE GROUP THAT SAW THE
LOW RISK OCCUPATIONALS, PRIVACY
FRIENDLY POLICIES AND ONE GROUP
OF THESE SAW HIGH RISK POLICIES
AND WE HAD THE SUBGROUPS WHERE
WE HAD POLICIES HIDDEN BEHIND A
LINK WHERE WE HAD THIS EXCLUSIVE
PRESENTATION WHERE WE HAD THIS
IMBEDDED POLICY AND AS A SEVENTH
GROUP WE HAD A CONTROLLED GROUP
WHERE THERE WAS NO POLICY TEXT
AT ALL INCLUDED.
AS I TOLD YOU WE DIDN'T TELL THE
PEOPLE IT'S ABOUT PRIVACY POLICY
BUT ABOUT TESTING THE AP.
SO WE, THEN DID SOME DISTRACTION
QUESTIONS, ASKING THEM HOW DID
YOU LIKE OUR AP?
WOULD WOULD YOU RECOMMEND IT TO
YOUR FRIENDS?
SUDDENLY, WE ASK PEOPLE FOR
RECALL, DO YOU RECALL WHERE THE
AP SAVES YOUR DATA?
DO YOU RECALL IF THE AP USES A
CENSOR, SO PEOPLE HAD TO TAKE A
LITTLE BIT OF A QUIZ RIGHT AFTER

AT THE END OF OUR EXPERIMENT,
AND THAT WAS BASICALLY THE
ESSENCE OF OUR EXPERIMENTS IN
ORDER TO SEE IF THE STUFF IS
REALLY WORKING BECAUSE A LOT OF
PREVIOUS EXPERIMENTS TOLD PEOPLE
TO READ THE POLICIES BUT OUR
ASSUMPTION IS THAT BASICALLY,
THE BEHAVIOR IS VERY DIFFERENT
IF AND NOR NATURAL IF YOU'RE NOT
TELLING PEOPLE TO READ THE STUFF
BUT STILL ASK THEM TO RECALL THE
INFORMATION.
SO IN THE END, I NOW SHOW YOU
THE RESULTS ON THE NEXT SLIDE.
WE ASKED EIGHT QUESTIONS IN
TOTAL.
PEOPLE HAD FOUR POSSIBLE ANSWERS
OF ONLY WHICH ONE WAS CORRECT.
I TOLD YOU PEOPLE COULD ALSO
GUESS.
WE HAD TO ACCOUNT FOR THE
GUESSING EFFECT THAT'S WHAT OUR
CONTROL WAS GOOD FOR WHERE NO
PRIVACY POLICY WAS INCLUDED SO
THIS WAS SOME KIND OF A BASELINE
FOR GUESSING IF PEOPLE DON'T
REMEMBER ANYTHING, THEY OH
PROBABLY HAVE A SCORE OF 2.5
CORRECT ANSWERS.
LEFT-HAND SIDE YOU SEE THE
RECALL SCORE, WHICH IS ALREADY
ACCOUNTS FOR THIS GUESSING
EFFECT, SO YOU COULD ALSO SAY
THIS IS BASICALLY TRUE
KNOWLEDGE.
PEOPLE REALLY REMEMBER STUFF, SO
MINUS, THE ALREADY ACCOUNTED FOR
THE GUESSING EFFECT AND AS YOU
CAN SEE IN CLICK CONDITION,
PEOPLE DON'T REMEMBER ANYTHING.
AND THAT'S EASY TO EXPLAIN
BECAUSE SIMPLY NOBODY CLICKED ON
THE LINK, OF, IT WAS LIKE 800

PEOPLE IN THIS CONDITION,
BASICALLY NOBODY -- OR I THINK
16 PEOPLE CLICK THE LINK.
HOWEVER, IN THE EXCLUSIVE
CONDITION, WHEN IT'S VERY, VERY
BOLD EVERYBODY HAD TO SEE IT,
PEOPLE START TO REMEMBER STUFF.
SO FOR EXAMPLE, IN THE PRIVACY
FRIENDLY CONDITION, PEOPLE
REMEMBERED TO COULD ANSWER TWO
QUESTIONS CORRECTLY AND IN THE
PRIVACY INTRUSIVE CONDITION, IT
WAS CLOSE TO THREE ANSWERS MADE
CORRECTLY.
THE IMBEDDED CONDITION WAS LESS
EFFECTIVE.
SO WHEN THE STUFF -- WHEN THE
PRIVACY INFORMATION WAS IMBEDDED
BELOW OTHER INFORMATION, THE
RECALL SCORE DECLINED BUT STILL
MORE EFFECTIVE THAN PLACING IT
BEHIND A LINK.
ON THE RIGHT-HAND SIDE YOU'LL
SEE THE TIE IN THAT THE
PARTICIPANTS SPEND IN THE
CONDITIONS AND YOU'LL SEE THEY
ACTUALLY SPEND MORE TIME IN
CONDITIONS WHERE THEIR PRIVACY
INFORMATION WAS PRESENTED IN A
MORE SALIENT WAY WHICH
DEMONSTRATE PEOPLE ACTUALLY
SPENT TIME READING THE
INFORMATION, WHICH EXPLAINS THE
RECALL THAT WE SAW IN THE RECALL
SCORE.
WHICH BRINGS US TO THE LAST
SLIDE WHAT DID WE LEARN IN THIS
EXPERIMENT?
BASICALLY, WE CONCLUDE THAT THE
CONCISE AND SHORT PRIVACY
NOTICES ARE VERY PROMISING
APPROACH TO INCREASE USER
AWARENESS IN TERMS OF RECALL
SALIENT SEE HAS A HUGE PREP

EFFECT ON THE AWARENESS OF THE DATA PRACTICES THAT IS MEASURED BY MEANS OF RECALL PERFORMANCE IN OUR EXPERIMENT, SO IF YOU MAKE IT NOT VERY SALIENT AT ALL, NO EFFECT, IF YOU MAKE IT HIGHLY SALIENT YOU HAVE WHAT WE WOULD SAY HUGE EFFECT GIVING OR TAKING INTO ACCOUNT THAT BASICALLY NOBODY OR A LOT OF PEOPLE ARE PROBABLY NOT EVEN INTERESTED IN THIS INFORMATION.
SO SALIENT SEE HAS A BIG EFFECT.
MAKING IT BOLD IS BETTER THAN JUST EMPTY BEDDING IT AND IN COMPLIANCE PRESENT WITH OUR EXPECTING, IF IT'S RISKY, PEOPLE RECALL IT BETTER.
WE HAVE CHOOSE A VERY SPECIFIC CONTEXT, IT WAS ALSO JUST A LAP EXPERIMENT, SO NOT A FIELD EXPERIMENT THAT WOULD HAVE TO BE DONE IN THE FUTURE, REALLY TRYING IT OUT.
BUT YOU COULD ALSO SAY THAT OUR CONCLUSION IS THAT THIS IS VERY SIMILAR TO WHAT PROBABLY PEOPLE IN MARKETING RESEARCH WOULD CONFIRM.
SO IT IS POSSIBLE TO BASICALLY MAKE RELEVANT INFORMATION LIKE PERCEIVED BY PEOPLE, SO IT'S NOT A NATURAL LAW THAT PRIVACY POLICY AND THE INFORMATION THAT'S INSIDE IS NOT PERCEIVED BY PEOPLE SO IT IS POSSIBLE IF YOU REALLY WANTED TO DO THIS, TO PRESENT THEM IN A FORM THAT IS PERCEIVABLE BY THE PEOPLE.
THANK YOU VERY MUCH.
SDDHANT
>> I WANTED TO FOLLOW UP TO START ON YOUR DISCUSSION OF

BREVITY AND SORT OF HOW SHORT POLICY TEXT CAN BE USEFUL PRIVACY AWARENESS, CAN YOU ELABORATE ON THAT AND HOW IT CAN HELP USERS
>> YES, MAYBE WE CAN SWITCH TO THE SLIDE AGAIN, I'M NOT SURE IF THE SLIDE IS STILL OPEN.
I'M PRETTY SURE THAT YOU ALL HAVE SEEN THIS WHAT'S UP AP? THEY HAVE EXACTLY USE THE SAME APPROACH, THEY PICKED UP INFORMATION, THEY CONSIDER RELEVANT AND I'M PRETTY SURE A LOT OF PEOPLE WERE ABLE TO CONCEIVE THIS INFORMATION IF PRESENTED IN THIS FORM.
IT'S BASICALLY STILL A BIG CHALLENGE WHAT INFORMATION TO PICK AND WHAT INFORMATION YOU CAN CHOOSE IN ORDER TO PRESENT IT, YOU CANNOT SIMPLY COMPRESS YOUR LIKE TEN-PAGE PRIVACY POLICY INTO LIKE FIVE SENTENCES FOR SURE, SO ONE OF THE MAIN CHALLENGES WILL BE WHAT INFORMATION IS RELEVANT TO THE PEOPLE IF YOU WANT TO USE THESE PERFORMANCE, AND ALSO, PEOPLE IN MARKETING RESEARCH HAVE ANSWER THIS QUESTION, SO IT REQUIRES CONTINUED RESEARCH PROBABLY ALL THE REGULATORS HAVE A SAY WHAT IS RELEVANT BUT BASICALLY, YOU HAVE TO DISCOVER NOW WHAT'S RELEVANT IN ORDER TO DISPLAY THIS IN AN ADEQUATE TEXT RELAY FORM.
>> FOLLOWING UP ON THAT, HAVE YOU FOUND IN YOUR OWN RESEARCH HOW CONSUMER DECIDE WHAT INFORMATION IS RELEVANT IN THOSE TEXTS?
>> YES.

SO ONE THING THAT IS IMMEDIATELY
CAME OUT OF THIS PAPER OBVIOUSLY
INFORMATION OR STUFF THAT IS
RISKY OR POTENTIALLY RISKY IS
CONSIDERED TO BE RELEVANT.
AND RESEARCH OFF OF US SHOWN
IT'S MOSTLY TO DO WITH THIRD
PARTY DATA SHARING.
THAT'S FOR EXAMPLE, ONE
CLASSICAL RISK THAT IS SEEMS TO
BE RELEVANT FOR.
-- SEEMS TO BE A RELEVANT
CONCERN THAT'S ONE EXAMPLE OF
WHAT PEOPLE WOULD PROBABLY
CONSIDER AS A RELEVANT PRIVACY
INFORMATION.

ARE.
>>>
>> YOU MENTIONED EARLY THE ISSUE
OF ICONS AND THE USE OF ICONS BY
ORGANIZATIONS.
THAT'S SOMETHING WE DEFINITELY
15 GREATER INCREASE OF IN TERMS
OF USING ICONS IN CONNECTION
WITH PRIVACY NOTIFICATIONS.
MAYBE YOU CAN TALK A LITTLE HOW
TEXT CAN BE COMBINED WITH ICONS
AND WHAT YOU -- WHAT YOUR
RESEARCH FOUND THERE.
>> YES.
SO WE HAVEN'T -- ON OUR OWN
RESEARCH ABOUT THIS TOPIC OF
USING ICONS BUT THERE'S A LOT OF
RESEARCH ALREADY THAT'S STARTING
TO GET MORE RESEARCH ON THESE
ICONS AND BASICALLY, YES,
COMBINE THEM, THIS IS ALSO WHAT
COMPANIES DO.
BUT I WOULD SAY THAT YOU CAN USE
THEM BOTH WAYS.
YOU CAN USE THEM TO WARN PEOPLE
TO GET THEIR ATTENTION, YOU CAN
ALSO USE THEM TO MAKE A COZY

ATMOSPHERE SO THEY PROBABLY
WOULDN'T EVEN READ THE TEXT.
IT'S LIKE SIGNS ON THE STREET
THAT TELL YOU ABOUT THE TEMPER
LIMIT, YOU CAN IMAGINE DIFFERENT
FORMS OF DESIGN WITH THE SAME
INFORMATION, BUT WITH DIFFERENT
OUTCOMES.
SO THIS REALLY NEEDS
INVESTIGATION, BECAUSE I WOULD
ARGUE THAT YOU CAN HAVE ANY KIND
OF EFFECT LIKE REMEMBER THIS
APPLE SIGN OF THESE TWO SHAKING
HANDS WOULD BE INTERESTING TO
SEE IF PEOPLE -- IF THIS ALREADY
RAISES TRUST AND PROBABLY NOBODY
EVER READS THE INFORMATION BELOW
ANYMORE.
SO THAT'S AN INTERESTING
QUESTION TO STUDY BUT GENERALLY,
I THINK IT'S POSSIBLE TO COMBINE
THEM, COMBINE WITH ICON AND
EFFICIENT COMBINATION.
>> THAT'S AN INTERESTING
EXTENSION OF WHAT YOU'VE BEEN
DOING.
ARE -- YOU'VE TALKED A LOT ABOUT
THIS USE OF SHORT POLICY TEXTS
ANDIS TELLING THE INFORMATION,
DO YOU HAVE A VIEW ON WHAT
TRADITIONAL POLICY DISCLOSURE
DOCUMENTS ARE NEEDED ANY LONGER.
>> MY ASSUMPTION IS THAT THEY
ARE JUST NEEDED BY LAW .
SO LIKE I'M NOT -- I'M NOT A
LAWYER.
THE COMPANIES I'VE BEEN TALKING
TO WOULD TELL ME THAT IT'S
REQUIRED TO HAVE ONE.
IT'S -- IT'S REQUIRED TO HAVE
TERMS AND CONDITIONS BUT THEY
ARE AWARE IT'S NOT AN EFFECTIVE
INFORMATION MEASURE.
SO WHAT YOU COULD DO IS STILL

HAVE YOUR OLD LONG POLICY TEXT REQUIRED BY LAW, BUT USE MORE LIKE SALIENT SHORTER USER FRIENDLY, USER UNDERSTANDABLE WAYS FOR THIS PART OF INFORMATION THAT SHOULD BE REALLY PERCEIVED.
SO I THINK WE WILL END UP WITH A COMBINATION AND THAT'S, FOR EXAMPLE, ALREADY WHAT APPLE AND ALSO WHAT'S AP FACEBOOK DID WAS JUST USING THEM IN COMBINATION WITH THE POLICIES THAT THEY HAVE ALREADY.
TIKTOK WOULD BE A NICE EXAMPLE OF HAVING KIDS FRIENDLY PRIVACY S3 POLICIES LIKE THEY ARE STILL THERE BUT KID FRIENDLY AP BUT PRIVACY POLICY IS MORE LOYAL FRIENDLY ALTHOUGH THEY MADE IT EASIER BUT ALREADY BUT I THINK YOU CAN COMBINE IT VERY GOOD WITH LONG POLICY TEXTS.
>> DO YOU HAVE VIEW HOW TO ENFORCE OR KIND OF INSURE THAT MORE COMPANIES OR ORGANIZATIONS ARE USING THESE SHORT SALIENT POLICY TEXTS THAT YOU FOUND -- THAT YOUR RESEARCH FOUND TO BE EFFECTIVE IN REACHING CONSUMERS?
>> YES.
THAT'S A VERY GOOD AND INTERESTING QUESTION.
IT'S VERY DIFFICULT TO ENFORCE THIS.
THERE ARE FOR SURE COMPANIES THAT ARE HAVE AN INTEREST TO CREATE AWARENESS OF THE PRIVACY PRACTICES.
IF IT HAS TO BE OR IF IT'S DONE VIA REGULATION, I GUESS IT'S -- IT'S GETTING COMPLEX.
YOU PROBABLY NEED VERY PRECISE LIKE FOR EXAMPLE, DESIGN

RECOMMENDATIONS ON WHAT HAS TO
BE PRESENTED BECAUSE OTHERWISE,
YOU WILL ALWAYS FIND WAYS AROUND
DESIGN WAYS YOU CAN BASICALLY
YOU CAN BEAT SALIENT WITH
SALIENTS BY MAKING SOME OTHERS
SEEM MORE SALIENT, THAT'S WHAT
WE ALSO DEMONSTRATED, SO IF YOU
IMBEDDED THE TEXT BENEATH VERY
NICE IMAGE OF LANDSCAPE, NOBODY
WILL READ THE TEXT ANYMORE.
SO BASICALLY IF YOU REALLY WANT
TO REGULATE THESE TOPICS, YOU
WOULD HAVE TO LOOK AT OTHER
AREAS OF REGULATION, FOR
EXAMPLE, EUROPE, WE HAVE
DISCUSSED NUTRITION LABELS THAT
ARE BASICALLY VERY HIGHLY
STANDARDIZED ON A PIXEL LEVEL,
YOU WOULD HAVE TO DO THIS IN
ORDER TO ENFORCE THIS.
>> THANKS NICO.
THAT'S ALL I HAVE FOR NOW.
I'D LIKE TO -- I APPRECIATE YOUR
-- THIS WAS A VERY INTERESTING
PRESENTATION.
I APPRECIATE THE TIME YOU'VE
TAKEN TO ANSWER MY QUESTIONS.
I'M NOW GOING TO TURN IT OVER TO
SIDDHANT ARORA TO MAKE HIS
PRESENTATION
>> HI, EVERYONE, I'M SIDDHANT
ARORA FROM CONCURRENT AGREE
MELON, I'M HERE TO GIVE A
PRESENTATION ON AUTOMATIC
EXTRACTION OF OPT OUT STATEMENTS
FROM PRIVACY POLICY.
CONDUCTIBLE AS PART OF THE
USABLE PRIVACY PROJECT.
CONCERNS PRIVACY THESE CHOICES
ALLOW USERS TO OPT OUT OF
CHOICES SENDING THEM E-MAIL
COMMUNICATION, ADVERTISEMENTS
BASED ON BEHAVIORS AND SHARING

FIRST NAME INFORMATION WITH
THIRD PARTIES BUT THESE OPTIONS
OFTEN WILL BE IN POLICY TEXT
MANY USERS DO NOT KNOW THEY EVEN
DO.
OUR GOAL IS TO HELP THESE USERS,
IN THIS WORK, WE WILL DO OUR
BEST WE CAN GET COMPUTER THESE
PRIVACY POLICIES.
WE HAVE PREVIOUSLY HAD SOME
SUCCESS IN AUTOMATICALLY
EXTRACTING USEFUL INFORMATION IF
PRIVACY POLICIES WE ASKED
WHETHER SIMILAR APPROACHES COULD
BE USED TO AUTOMATICALLY START
OPT OUT CHOICES IN PRIVACY
POLICIES AND MAKE THEM MORE
READY BELIEVE ACCESSIBLE AND
USABLE TO END USERS.
NEXT SLIDE, PLEASE.
>> WHILE MANY WEBSITES OFFER
USERS CHOICES TO OPT OUT OF SOME
DATA COLLECTION AND USE
PRACTICES.
MOST CHOICES ARE BURIED DEEP IN
THE TEXT OF LONG JARGON FILLED
POLICY POLICIES AND NEVER SEEN,
DIFFERENT GRANT USERS THE RIGHT
TO OPT OUT RELYING ON COLLECTION
OF USE OF DATA INCLUDES THE
RIGHT TO OPT OUT OF HAVING ONE
DAY TODAY SHARED WITH PARTIES
FOR DIFFERENT PURPOSES, THE
RIGHT TO OPT OUT OF RECEIVING
MARKETING E-MAILS COOKIES AND
MORE BUT DON'T OFFER EASY ACCESS
TO THESE CHOICES EFFECTIVELY
DEPRIVING USERS OF RIGHTS, TO
HELP MAKE MORE ACCESSIBLE, A
TEAM OF RESEARCHERS FROM
CARNEGIE MELON UNIVERSITY
DEVELOPED A BROWSER EXTENSION
CALLED OPT OUT EASY, WHICH USES
MACHINE LEARNING TECHNOLOGY TO

AUTOMATICALLY TO FIND OPT OUT CHOICES FOR USERS AS THEY BROWSE.
OPT IS'S AVAILABLE TO BOTH CHROME AND FIRE FOX, BY CLICKING ON THE ICON, USERS ARE PRESENTED WITH OPT OUT LINKS FOUND PRIVACY POLICY OPTING THEM ANALYTICS OR MARKETING E-MAILS, START PRACTICING YOUR RIGHT WITH OPT OUT EASY TODAY.
>>> THE MAJOR RESEARCH ARE THE FOLLOWING.
WE BUILD MACHINE LEARNING CLASSIFIERS TO OPT OUT STATEMENTS FROM THE PRIVACY POLICIES BUILD A BROWSE EXTENSION THAT SHOWS RESULTS FOR OPT OUTS, THE BROWSE EXTENSION IS NOT PUBLICALLY AVAILABLE AND CAN BE DOWNLOADED FROM THE LINK SHOWN ON THE SLIDE.
ANOTHER BENEFIT OF THE AUTOMATIC CLASSIFICATION APPROACH PRESENTED IN THIS BOOK IS THAT IT ACTUALLY ENABLES PEOPLE TO MORE SYSTEMATICALLY ANALYZE OPT OUT DEMOGRAPHICS WITHIN AND ACROSS DIFFERENT WEBSITES.
THE PRIVACY POLICIES ARE PRESENTED ON PAGES BUT THERE ARE NO STANDARD LOCATION FOR THE PRIVACY POLICIES.
WE BUILD A MODEL THAT FOUND A PAGE CONTAINING A PRIVACY POLICY FOR PUT THE GIVEN WEBSITE, WE WERE ABLE TO OBTAIN 236 WEB PAGES, THE TEXT OF THE PRIVACY POLICY INTO WHAT WE CALL SEGMENTS.
WE RELIED ON LINKS SERVICES LIKE DAA AND NAI TO AUTOMATICALLY IDENTIFY THESE OPT-OUTS BEFORE THE MACHINE LEARNING CLASSIFIERS

FOR THE REMAINING HYPER LINKS
MORE DIFFICULT TO IDENTIFY AT
OPT OUT.
TO CLAIM THESE CLASSIFIERS WE
GOT 2,692 HYPER LINKS.
UP UNTIL THIS POINT, WE HAVE
DISCUSSED ABOUT THE PIPELINE WE
BUILT IN ORDER TO COLLECT THE
ANNOTATIONS.
ALTHOUGH THAT INFORMATION IS
USEFUL, IT'S OF FAIR AMOUNT
IMPORTANCE TO UNDERSTAND OPT
OUT.
HENCE WE DECIDED TO DO A
ANALYSIS OF THE OPT OUT CHOICES.
DOING THE DATA COLLECTION
PROCESS, WE WOULD ANNOTATE EACH
HYPER LINK WITH UP TO TWO DATA
PRACTICE CATEGORIES.
THESE CATEGORIES WERE BASED ON
PRIVACY PROPOSED IN EUROPE LIKE
CCPA AND GP DR.
SOME ARE REQUIRED BY LAW.
WE CLASSIFIERS WHERE WE WOULD
GENERALLY FEATURE BASED ON THE
SEGMENT TEXT, DUI OF A HYPER
LINK AND THE ANCHOR TEXT
ASSOCIATED WITH THE HYPER LINK
TO AUTOMATICALLY CATEGORIZE A
HYPER LINK AS OPT OUT.
IN THE EXAMPLE THAT WE SEE IN
THIS SLIDE, WE CAN SEE HOW THE
HYPER LINK TEXT GO TO OUR
SETTINGS AND THE SURROUNDING
TEXT DISCUSSING MANAGING OUR
PREFERENCES CAN HELP TO CLASSIFY
THE GIVEN HYPER LINK AS OPT OUT.
CLASSIFIERS WILL BE A PRECISION
-- 93 PERSONS WERE IN FACT, OPT
OUT AND THE RECALL OF 0.90
THAT'S A CLASSIFY ER
SUCCESSFULLY, 90 PERSONS OF THE
OPT-OUT HYPER LINK.
AFTER BUILDING CLASSIFIERS,

WHICH ARE ABLE TO CATEGORIZE THE OPT-OUTS, INTO DIFFERENT DATA PRACTICES, WE WANTED TO STUDY THE DEMOGRAPHICS OF THESE OPT OUTS.
HENCE WE PERFORM AN ANALYSIS ON AROUND 7,000 PRIVACY POLICIES, HERE ARE THE KEY QUESTIONS YOU WANT TO ANSWER.
OUT OF THE WEBSITES WHICH WERE WE ANALYZED HOW MANY WEBS HAD OPT-OUTS?
WE CAN SEE THAT MOST OF POLICIES DO NOT HAVE ANY OPT-OUTS, WHICH IS CONSISTENT WITH THE PREVIOUS FINDINGS.
WHAT IS THE AVERAGE NUMBER OF OPT-OUTS PER WEBSITE AND HOW IS IT RELATED TO THE POPULARITY OF THE WEBSITE?
SO IN THE GRAPH THAT WE SEE ON THE SLIDE WE SEE THAT THE MEAN NUMBER OF OPT-OUTS BASED ON THE WEBSITE, WE OBSERVED THAT HIGHER RANKED WEBSITES HAD MORE OPT-OUTS IN THEM.
WE ALSO WANTED TO UNDERSTAND THE DISTRIBUTION OF OPT-OUT CATEGORIES.
THIS GRAPH SHOWS THE DISTRIBUTION OF VARIOUS OPT-OUT CATEGORIES WE HAVE RECOGNIZED FOR 200 MOST POPULAR WEBSITES.
DISTRIBUTION OF OPT-OUT HYPER LINKS ARE SKEWED BUT MOST OF THE WEBSITES WHO ARE ADVERTISING OPT OUT HYPER LINKS.
IT WAS ALSO OBSERVED THESE TRENDS WAS SIMILAR IRRESPECTIVE OF THE WEBSITE'S POPULARITY.
UP UNTIL NOW, WE HAVE DISCUSSED THESE FINDING OF OPT-OUTS AND DOING AN ANALYSIS OF THE OPT-OUT CATEGORIES ON THE WEB BUT OUR

WORK WILL HAVE MORE VALUE WHEN
WE CAN PROVIDE THIS TECHNIQUE AS
A SERVICE TO THE END USER, SO
THAT PRIVACY.
IN OUR OPINION, BEST WAY WE
COULD MARKET THE SERVICE IS WITH
BROWSER EXTENSION, SO WE BUILD
AN EXTENSION CALLED OPT OUT
EASY, WHICH WOULD MAKE IT EASIER
FOR PEOPLE TO FIND AND OPT OUT
OF DATA PRACTICE CONTROLS.
THIS IS PUBLICALLY AVAILABLE
WITH THE DOWNLOADING MENTIONED
ON THE SLIDE AND WE ENCOURAGE
YOU TO DOWNLOAD IT.
SO IN THIS EXTENSION, WE USED A
DESIGN APPROACH WITH FOR
IMPORTANT IN THE END.
THE FIRST ONE SHOWS YOU THE
OPT-OUT PRACTICES AND THE KIND
OF OPT-OUTS FOR A GIVEN WEBSITE.
THE SECOND SCREEN DISPLAYS THE
LIST OF WEBSITES YOU VISITED AND
ALL THE OPT-OUT CONCLUDES, WHICH
ARE ASSOCIATED FOR THAT
PARTICULAR WEBSITE.
IT WILL SHOW YOU THE OPT-OUT
CONTROL WHICH YOU HAVE VISITED
IN BLUE.
AND IT PROACTIVELY ENCOURAGES
YOU TO TAKE ACTION AND OPT OUT
OF UNWANTED DATA PRACTICES.
WE ALSO HAVE A HELP PAGE IN THE
EXTENSION THAT WILL SHOW USERS
THE WORKING OF THE PLUG IN.
THE ANALYZED PRIVACY POLICIES
ARE STORED IN THE DATABASE.
ONLY SHOW THE RESULTS TO THE
USERS.
HOWEVER, OPT OUT ALSO ALLOW USER
TO REQUEST FOR WEBSITES THAT
HAVE NOT BEEN ANALYZED YET.
WE THEN THE ANALYSIS TO POPULATE
THE RESULTS FOR THOSE WEBSITES

AND SHOW THEM LATER.
AS WE HAVE SEEN, OUR TECHNOLOGY DOES A PRETTY GOOD JOB AT EXTRACTING OPT OUT CHOICES BUT HOW USEFUL IS TO BROWSE THE EXTENSION WE HAVE OPT OUT.
TO ANSWER THIS WE DECIDED TO RUN A HUMAN SUBJECTS STUDY.
WE PERFORMED A CONTROL EXPERIMENT WITH EIGHT PARTICIPANTS.
THE GROUP WAS EXPLAINED AND GIVEN ACCESS TO THE BROWSER EXTENSION.
SO WE ASKED USERS TO PERFORM FIVE OPT-OUT TASKS ON FOUR DIFFERENT WEBSITES.
THIS TASK WAS TO OPT OUT OF A DATA PRACTICE CATEGORY BASED ON THE PROMPT WHICH THE SUBJECT WAS GIVEN.
WE SEEN THAT THE TIME TAKING FOR OPTING OUT IN ALMOST ALL TASKS IS MUCH MORE IN THE CONTROL GROUP THAN THE OTHER GROUP.
THE SUCCESS RATE IS HIGHER FOR THE ACHIEVEMENT GROUP OR THE CONTROL GROUP.
THIS IS BECAUSE THE USERS GET FED UP OF SEARCHING FOR AN OPT OUT AND EVENTUALLY DECIDE TO GIVE UP.
HERE ARE SOME OTHER DISCUSSION POINTS FROM OUR USER STUDY.
USERS ARE OFTEN UNAWARE OF AVAILABLE OPT-OUT CHOICES AND SOMETIMES LACK THE NECESSARY KNOWLEDGE NEEDED TO OPT OUT SUCCESSFULLY.
THE OPT-OUT HYPER LINKS ARE OFTEN BROKEN AND TAKE TOO MUCH TIME TO RESPOND.
WHICH MAKES THE USER GIVE UP AND QUIT OUT OF THE OPT IN PROCESS.

DUE TO ALL THESE REASONS, WE
BELIEVE THAT PRIVACY LAWS SHADS
PUT PRESSURE TO INSURE THAT THE
SERVICES ARE ALWAYS AVAILABLE IN
THE FORM OF STANDARDIZED API's.
THE FINAL TAKE AWAY FROM THIS
PRESENTATION THAT WE HAVE
DEVELOP TECHNIQUES CAPABLE OF
IDENTIFYING OPT OUT TEXT FROM
PRIVACY POLICIES.
WE PRESENTED A BROWSER
EXTENSION, WHICH IS VALUABLE IN
GOOGLE CHROME AND FIRE FOX.
WE ENCOURAGE YOU TO DOWNLOAD THE
BROWSER EXTENSION RIGHT NOW AND
TAKE BROWSING IN YOUR OWN HANDS,
THANKS FOR YOUR ATTENTION.
CORE.
>>> THANKS A VERY INTERESTING
TOOL YOU PUT TOGETHER FOR US.
I WANT TO START BY ASKING YOU AT
THAT POINT YOU RAISED A COUPLE
OF SLIDES AGO WHICH IS FROM A
REGULATORY STANDPOINT, YOU KNOW,
WE HERE AT THE FTC, WHAT DOES
YOUR RESEARCH SUGGEST ABOUT
FUTURE REGULATIONS FOR OPT-OUT
CHOICES FOR USERS?
>>
>> REALLY GOOD QUESTION, OUR
MAKES THREE SUGGESTIONS, FIRST
IS THAT THE PRIVACY LAWS, PUT
PRESSURE TO INSURE THESE
SERVICES ARE AVAILABLE IN THE
FORM OF STANDARDIZED API's LIKE
I TALKED ABOUT EARLIER IN OUR
USER STUDY, WE OBSERVED THAT NOT
EVERY WEBSITE OFFERS THE SAME
NUMBER OF OPT-OUTS AND THESE
OPT-OUT HYPER LINKS ARE OFTEN
BROKEN AND TOOK TOO MUCH TIME TO
RESPOND, OPENED A DIFFERENT
LEVEL WHICH WOULD FINALLY SHOW
THAT THE SERVICE IS TEMPORARILY

UNAVAILABLE.
SO BECAUSE ALL OF THE WAITING PERIOD THE USERS EVENTUALLY JUST GIVE UP AND QUIT OUT OF THIS OPTING OUT PROCESS.
SO YOU DO ALL THESE REASONS DESPITE OUR CLASSIFIERS HAVING VERY HIGH PRECISION, AND RECALL, IT'S OFTEN DIFFICULT FOR THE END USERS TO OPT OUT.
SO WE BELIEVE WE SHOULD NOT HAVE TO RELY ON MACHINE LEARNING BUT THIS OPT-OUT LINKS SHOULD BE READY TO DISCOVER IN THE FORM OF STANDARDIZED APE's.
ALSO, ONCE WE HAVE THESE API's USER WOULD NO LONGER NEED TO DO THIS FOR WEBSITE, WEBSITE BUT CAN ALWAYS CHOOSE TO OPT OUT BY SETTING UP PREFERENCES IN A PLUG-IN LIKE THE OPT-OUT EASY BROWSER EXTENSION.
IN ADDITION ABOUT OPT-OUT SETTINGS.
A LOT OF US DID PRIOR RESEARCH ON PEOPLE'S PREFERENCES TO OPT OUT PRACTICES FOR QUALITATIVE AND QUANTITATIVE SERVICES AND WHAT WAS OBSERVED WAS THAT WHICH ALLOW THESE PRACTICES WERE MORE BURDENSOME TO END USERS THAN THE SETTINGS CONTEXTLIZED BASED ON WEBSITE CATEGORIES, THAT'S ANOTHER INTERESTING ACTION.
AND IF IT WAS THERE NEEDS TO BE FOCUS ON NUDGING USERS TOWARDS MAKING BENEFICIAL CHOICES PERTAINING TO PRIVACY DECISION MAKING AND OUR LAB HAS DONE A LOT OF RE EARCH FOCUSED ON THAT.
I WANT TO TURN TO THE TOOL YOU CREATED AND FIND OUT HOW YOU PLAN TO CONTINUE DEVELOPING IT AND IMPROVING THE PERFORMANCE OF

YOUR SYSTEM AND FINDING AND
CATEGORIZING OPT-OUTS.
I KNOW YOU TESTED IT TO SOME
EXTENT BUT IT'S STILL -- HOW DO
YOU PLAN ON CONTINUING TO
DEVELOP IT?
>> THAT'S A REALLY NICE
QUESTION.
SO CLASSIFIED -- 2,700 HYPER
LINKS, WE BELIEVE IT WOULD
LIKELY IMPROVE THE PERFORMANCE
FOR CLASSIFIERS AND ALSO WE PLAN
TO DO FUTURE WORK ON ADDITIONAL
FEATURES TO IMPROVE THE
PERFORMANCE OF OUR SYSTEM.
ANOTHER ACTION WE CAN CURRENTLY
USE CLASSIFY ER WHERE THE
WEBSITE CONTAINS A PRIVACY
PRIVACY AND WHAT IS THE LOCATION
OF PRIVACY POLICY FOR THE
WEBSITE, SO IMPROVING THE
PERFORMANCE OF THIS CLASSIFY ER
CAN IMPROVE THE PERFORMANCE OF
OUR END SYSTEM IN EXTRACTING THE
OPT-OUT CHOICES .
ALSO, CURRENTLY, OUR METHODOLOGY
IS LIMITED TO EXTRACTING OPT-OUT
LINKS THAT USE.
ON MANUAL INSPECTION WE OBSERVED
THAT OPT-OUTS CAN ALSO OCCUR AS
LIKE, WITH JAVA STRIPPED THAT
WOULD AUTOMATICALLY, THE USERS,
SO WE PLAN TO EXTEND OR
METHODOLOGIES TO OPT-OUT LINKS
AS WELL.
ANOTHER THING WE'RE DOING GOING
TO TRY FOLLOWING HYPER LINKS AND
DOWNLOADING THE WEB PAGE THAT
THE HYPER LINKS LEADS TO WE
BELIEVE THIS COULD ALSO HELP IN
DETECTING IF THE GIVEN HYPER
LINK IS AN OPT-OUT OR NOT.
OPT
>>> SOUNDS LIKE A LOT OF THE

INTERESTING AVENUES TO EXPLORE
THERE.
WHAT KIND OF ANALYSIS IS
FACILITATED BY YOUR RESEARCH ON
AUTOMATICALLY IDENTIFYING AND
CHARACTERIZING OPT-OUTS?
WHAT OTHER ANALYSIS IS SORT OF
BORNE OUT OF YOUR RESEARCH?
>> SO THAT'S LOOK A VERY
INTERESTING QUESTION.
AND ONE OF THE BENEFITS THAT WE
THINK OF THIS AUTOMATIC
CLASSIFICATION APPROACH IS THAT
THEY COULD ACTUALLY ENABLE
PEOPLE AND REGULATORS TO MORE
SYSTEMATICALLY ANALYZE THE
OPT-OUT DEMOGRAPHICS WITHIN AND
ACROSS DIFFERENT WEBSITE
CATEGORIES LIKE BASED ON
DIFFERENT WEBSITE POPULARITY
WEBSITE SECTORS AND SO ON.
WE HOPE THAT MOVING FORWARD THIS
TYPE OF SYSTEMATIC ANALYSIS WILL
BE USED TO INFORM PUBLIC POLICY
DEBATES.
WE ALSO BELIEVE THAT OUR HAS A
LOT OF POTENTIAL IN BEING USED
IN COMPLIANCE, IN PARTICULAR,
LIKE WITH THE INTRODUCTION OF
THE CALIFORNIA CONSUMER PRIVACY
ACT, WHICH REQUIRES AN OPT-OUT
ON THE SALE OF -- IT WOULD BE
INTERESTING TO SEE IF WE CAN
EXTEND THE APPROACH AND DO A
SYSTEMATIC ANALYSIS LOOKING AT
THE PRESENT OPT-OUT HYPER LINK
FOCUSED ON THIS REQUIREMENT LIKE
ONE ARE IN COMPLIANCE WITH THIS
TOOL.
HOW DOES THIS COMPLIANCE WITH
LIKE WEBSITE POPULARITY AND
WEBSITE SECTORS AND SO ON?
WE ALSO ARE LOOKING INTO A MORE
EXTENSIVE STUDY HOW SECTOR RELY

REGULATIONS CAN AFFECT PRESENCE
OF OPT-OUTS LIKE U.S. FINANCIAL
ORGANIZATIONS ARE REQUIRED BY
THE (INAUDIBLE) TO HAVE THE
OPT-OUT NOTICES.
AND FUTURE WORK MIGHT EXAMINE
THE JURISDICTION UNDER WHICH
DIFFERENT SITES AND TO WHAT
EXTENT DO THESE AFFECT THE
NUMBER AND TYPE OF OPT-OUTS.
FOR EXAMPLE, WE'RE CURRENTLY
LOOKING AT THE U.S. AND GERMAN
FOR SAME WEBSITE AND TRYING TO
ANALYZE HOW DO THE DIFFERENT
NUMBER AND TYPE OF OPT-OUTS AND
HOW CAN THIS BE --
SPECIFICATIONS LIKE DPIU AND
CCPNU.
>> FINALLY I JUST WANTED TO
ASKING YOU IF YOU COULD, IF YOU
COULD REMIND US IS THE -- IS
YOUR EXIGENT OPT-OUT EASY, IS IT
AVAILABLE TO PUBLIC AND CAN I
USE IT NOW?
>> YES, YOU CAN.
SO THE OPT-OUT IS PUBLICALLY
AVAILABLE AS THE BROWSER
EXTENSION, WHICH IS GOOGLE
CHROME AND FIRE FOX AND WE
STRONGLY ENCOURAGE YOU TO
DOWNLOAD THE EXTENSION NOW AND
TAKE MATTERS IN YOUR OWN HANDS.
THANK YOU.
>> THANK YOU.
SIDDHANT.
THAT WAS A REALLY -- THAT'S JUST
A REALLY INTERESTING TOOL THAT
YOU'VE CREATED FOR PEOPLE TO
EXPLORE.
I'M NOW GOING TO TURN TO CAMERON
KORMYLO TO PRESENT HIS PAPER.
CAMERON?
>> THANK YOU, DANIELLE.
NEXT SLIDE.

PLEASE.
AS DANIELLE SAID, MY NAME IS CAMERON KORMYLO I'M A THIRD YEAR PHD STUDENT AT VIRGINIA TECH.
AND MY CO AUTHOR IN THIS PAPER AND VIRUS IS DR. TERESA ALSO OF VIRGINIA TECH, STUDIES AND INSPIRED MY INTEREST IN ECONOMICS OF PRIVACY.
SO THE PROBLEM THAT WE ARE ADDRESSING IN OUR PAPER KIND OF AROSE OUT OF THIS SORT OF FRIGHTENING REALITY THAT IS CURRENT STATE OF ONLINE CONSENT.
AS YOU CAN SEE, I CHOSE MY BACKGROUND TODAY TO BE THE BRIDGE IN PARIS MORE COMMONLY KNOWN AS THE LOVE LOCK BRIDGE.
I FELT THIS WAS A PRETTY GOOD VISUALIZATION FOR THE STATE OF TODAY'S PRIVACY LANDSCAPE.
SO THE BRIDGE ITSELF, YOU CAN THINK OF IS REPRESENTING ONE'S OWN PERSONAL PRIVACY AND EACH LOCK IS ANOTHER DECISION NEEDS TO BE MADE.
DO I TURN THE KEY OR THROW IT INTO THE SET?
DO I CONSENT TO SOME ONLINE DATA PRACTICE OR NOT?
AS I'M SURE MANY OF YOU ALSO KNOW IN 2014, GUARDRAILS FROM THE BRIDGE BEGAN TO COLLAPSE UNDER THE WEIGHT OF THE LOCKS AND DETERIORATING THE SAFETY AND STRUCTURE OF THE BRIDGE ITSELF.
CONSENT RATES FOR THESE DECISIONS ARE ASTRONOMICALLY HIGH AND THE TOOLS THAT INDUSTRY OR REGULATION HAS USED TO KIND OF PREVENT THIS HAVE BEEN LARGELY IN EFFECTIVE.
THE AD CHOICES PROGRAM WHICH GIVES USERS THE ANTIBIOTIC TO

OPT-OUT OF BEHAVIORALLY TARGETED ADS WAS ONLY USED IN 0.23% OF ALL AMERICAN AD IMPRESSIONS AND THIS KIND OF PHENOMENON FOR MY IS SIMILARLY SUBSTANTIATED BY ACADEMIC RESEARCH AND THERE HAVE BEEN PAST PAPERS THAT HAVE SEEN ALMOST UNIVERSAL ACCEPTANCE TO PRIVACY POLICIES EVEN INCLUDING THE NAMING RIGHT FOR FIRST CHILD, ACCESS TO AIR SPACE ABOVE HOMES FOR DRONE TRAFFIC, AND SHARING ALL DATA WITH NSA.

AS YOU CAN SEE THIS IS, YOU KNOW, KIND OF A VERY STRONG AND FRIGHTENING PHENOMENON.

AND THE CAUSES OF THIS HAVE BEEN DISCUSSED AND DISPUTED THE LAST DECADE OR TWO.

SOME INDUSTRY PROFESSIONALS AND ACADEMICS SITE CONSUMER INDIFFERENCE PRIVACY CONCERNS MAY PEOPLE JUST AREN'T THAT CONCERNED ABOUT THEIR PRIVACY OR COMPARATIVELY HAVE HIGH VALUATIONS FOR THE ONLINE SERVICES AND THOSE VALUATIONS KIND OF OVERPOWER CONCERNS THEY DO HAVE FOR PRIVACY.

HOWEVER, A SIGNIFICANT PORTION OF RESEARCH CONVERGE AROUND THE IDEA THAT MOST CONSUMERS DO NOT ACTIVELY EVALUATE THE COST AND BENEFITS OF CONSENTING TO THESE ONLINE DATA PRACTICES.

THIS IS ESPECIALLY TRUE FOR MOST IMPORTANT PRIVACY DECISIONS OFTEN IMPLICIT AND DIFFICULT TO REVERSE WHILE BEING COVERED UP BY THE COMPLEXITY OF THE CHOICE PRESENTATION.

SO REGULATORS AND POLICY MAKERS LARGELY TAKEN NOTICE OF THESE CONCERNS THIS REFLECTED IN THE

ENACTMENT OF BROAD CHANGES AS
WELL AS MORE FEDERAL REGULATION
THAT IS LARGELY CHAMPIONED BY
OUR HOST TODAY.
WITH EACH NEW REGULATION PASSED
WE HAVE NEW OPPORTUNITIES FOR
RESEARCH.
HOWEVER, A LOT OF THE CURRENT
RESEARCH FOCUSES ON THE BROAD
POLICY EFFECTS.
AND IT'S NICE TO KNOW THAT YOU
KNOW, DPR AS A WHOLE HAS A
POSITIVE OR NEGATIVE EFFECT.
IN REALITY THESE PRIMARY EFFECTS
SEEM TO BE FURTHER BROKEN DOWN
AND DIFFERENTIATED, WE NEED TO
CONSIDER SPECIFIC TENANTS, WHAT
PARTS OF GPR, FOR EXAMPLE,
INCREASE AND DECREASE IT?
MORE SPECIFIC CONSIDERATION
FURTHER INFORM FUTURE REGULATION
AND ALLOW FOR MUCH MORE DETAILED
FORMULATION OF POLICY.
OUR WORK SPECIFICALLY ISOLATES
THREE TENETS OF GDPR, UNDERSTAND
INDIVIDUAL EFFECTS AS WELL AS
INTERACTIVE EFFECTS THEY MAY
HAVE WITHIN EACH OTHER, WE LOOK
THE CHANGE STRUCTURE.
THAT REQUIRES CONSENT IS
EXPLICIT BANS THE USE OF
IMPLICIT CONSENT.
OFTEN IN THIS CONTEXT WOULD
IMPLICITLY ALLOW FOR CONSENT.
WHILE REQUIRING A CONSUMER TO
MAKE AN ACTIVE CHANGE IF THEY
DECIDED THEY DID NOT WANT TO
CONSENT.
AND ACADEMIC LITERATURE THE
CONSIDERATION OF THIS TYPE OF
CHANGE AND CHOICE PRESENTATION
IS CALLED CHOICE ARCHITECTURE OR
HOW THE DESIGN OF A CHOICE CAN
DIFFER WHEN PRESENTED TO

CONSUMERS AND HOW THESE
DIFFERENCES IMPACT THE
SUBSEQUENT DECISION MAKING.
DEFAULT CHOICES AS DISCUSSED ARE
POPULAR TOOL OF CHOICE
ARCHITECTURE AND CAN TAKE
ADVANTAGE OF CONSUMER DECISION
BIAS SEES AND ENCOURAGE SOME
PARTICULAR OUTCOME.
SECOND WE CONSIDER REVERSIBLE
CONCERT REQUIRED BY ARTICLE
SEVEN, AND THIS DRASTICALLY RE
FIGURES THE STRUCTURE OF CONSENT
IN SUCH A WAY THAT CONSUMERS NOW
KNOW THAT THE CHOICE THEY'RE
MAKING IS NOT PERMANENT.
IT CAN BE RE VISITED AT A LATER
DATE AND WHILE THIS IS MEANT TO
GIVE INDIVIDUALS MORE CONTROL
OVER PRIVACY, THIS COULD ALSO
LEAD CONSUMERS TO VIEWING THE
CHOICES MAYBE LESS SERIOUS OR
LESS PRESSING AND THIS COULD
EVEN ENCOURAGE THEM TO BE MORE
LACKS WITH THEIR DECISION.
FINALLY WE LOOK AT A LARGELY
IMPLICIT CHANGE FROM GDPR
RESULTED IN CONSENT BEING HIGHLY
REPETITIVE THIS IS REPRESENTED
BY THE COUNTLESS LOCKS HERE ON
THE LABLOCK BRIDGE.
PREVIOUSLY PRIVATE PRIVACY
DECISIONS WERE HE CAN SAY
IMPLICATELY MADE.
AS WE'VE ALL SEEN ALMOST EVERY
INTERACTION WITH A WEBSITE IS
ACCOMPANIED WITH A COOKIE BANNER
ASKING CONSUMERS TO CONTINUESLY
MAKE CONSENT DECISIONS THIS HAS
THE POTENTIAL TO FURTHER
INFLUENCE CONSUMER CHOICE MAY
LEAD TO A SENSE OF FATIGUE WHERE
THEY'VE GIVEN IN CONSENT ALL THE
TIME OR DO THE OPPOSITE WHERE

THEY ADJUST THE BELIEF SYSTEM SLIGHTLY EACH TIME AND EVENTUALLY LEARN TO MAKE MORE INFORM DECISION.
NEXT SLIDE.
GIVEN THAT CONSIDERATION, WE CAN SUMMARIZE OUR RESEARCH GOALS AS FOLLOWS.
SO FIRST WE EVALUATE THE EFFECT OF CHANGING CHOICE, A ARCHITECTURE OR SPECIFICALLY THE DEFAULT CONSENT CHOICES ON THE OUTCOME OF CONSUMER PRIVACY DECISIONS.
SECOND, WE EXPLORE HOW REVERSE ABILITY AND REPEATED EXPOSURE IMPACT DECISION MAKING ACROSS THE DIFFERENT CHOICE ARCHITECTURES.
SO TO STUDY THIS, WE CAN CONDUCTED AN ONLINE EXPERIMENT THAT ASKED PARTICIPANTS TO MAKE A REAL PRIVACY DECISION.
WHERE THEY HAD TO DECIDE WHETHER OR NOT TO FOREGO ANONYMITY IN THE FACE OF A SENSITIVE DISCLOSURE, IT WAS STRUCTURED AS A TWO FACTOR, THREE BY THREE EXPERIMENT, TWO FACTORS WERE CHOICE ARCHITECTURE AND REVERSE ABILITY OF THE CHOICE AND PARTICIPANTS TOOK THE EXPERIMENT THREE TIMES WITH DIFFERENCES ONLY IN THE CONTEXT OF THE DISCLOSURES.
RESULTING IN A PANEL DATA STRUCTURE THAT ALLOWED FOR US TO CONSIDER THE EFFECTIVE OF THESE REPEATED PRIVACY CHOICES.
AS YOU CAN SEE IN THE TABLE HERE, PARTICIPANTS WERE EITHER IN A UNIVERSAL OPT-OUT THAT DEFAULTING THEM IN CONSENTING, ACTIVE CHOICE STRUCTURE THEY HAD

TO EXPLICITLY CHOOSE TO CONSENT
OR NOT TO.
OR A MORE PROTECTIVE OPT-OUT
STRUCTURE WHERE THEY WERE
DEFAULT I DO NOT NOT CONSENTING
AND HAD TO ACTIVELY CHANGE
DECISION IN ORDER TO CONSENT
ADDITIONALLY THEY WERE GIVEN
EITHER NO INFORMATION AS THE
REVERSE ABILITY OF THE CHOICE OR
EXPLICITLY TOLD THAT THE CHOICE
WAS EITHER REVERSIBLE OR
IRREVERSIBLE.
SO THIS IS KIND OF THE PROCEDURE
OF OUR EXPERIMENT PARTICIPANTS
WERE TOLD THEY WERE TAKING PART
IN A NUMBER OF SURVEYS THAT HAD
TO DO WITH SENSITIVE
INFORMATION, SUCH AS CRIMINAL
ACTIVITIES, SEXUAL HISTORY AND
ROMANTIC INVOLVEMENT.
THEY THIS MIMICS WHAT THEY WOULD
MAKE WHEN SIGNING UP OR SOCIAL
MEDIA SITE, ASKED FOR GENDER
RACE, GEOGRAPHIC INFORMATION
EVEN FORM OF ZIP CODES THEN
DIRECTED TO THE MAIN TREATMENT
AND THIS IS KIND OF WHERE THEY
WERE ASKED WHETHER OR NOT THEY
WOULD LIKE TO IN ESSENCE SIGN IN
TO THE RESEARCH PROFILE, WHICH
WOULD LINK THEIR SUBSEQUENT
DISCLOSURES BACK TO THEM.
SO THIS IMAGE HERE SHOWS A
PICTURE OF THE DECISION, WHERE
THE CHOICE IS REVERSIBLE.
WE TELL THEM THEY CAN CHANGE
THEIR DECISION AT ANY TIME.
AND IT'S PRESENTED AS AN ACTIVE
CHOICE, WHERE THEY HAVE TO CLICK
SIGN INTO THE RESEARCH PROFILE
OR CLICK SIGN IN AS GUEST WITH
NO OPTION DEFAULT, THEY WERE
DIRECTED TO A SURVEY THAT HAD

THE SENSITIVE DISCLOSURES I MENTIONED IF THEY CHOSEN TO LOG IN THE RESEARCH ID WAS LISTED IN THE TOP CORNER OF THE PAGE, MAKING THE VERY SALIENT THAT THE ANSWERS WERE LINKED BACK TO THEM.
AFTER THE SURVEY THERE WAS A TIME BUFFER IN THE FORM OF A CONTEXT SPECIFIC VIDEO THEY WERE ASKED TO WATCH BEFORE DIRECTING THEM TO THE NEXT OF THE THREE AS FAR AS I WAS WHERE THE CONSENTS DECISION WOULD BE PRESENTED AGAIN.
TO GET INTO A RESULTS.
FIRST RESEARCH GOAL WAS TO IDENTIFY THE EFFECTIVES OF CHANGING CHOICE ARCHITECTURE.
THERE'S A VERY SIGNIFICANT EFFECT OF THIS TREATMENT.
THOSE IN THE CONTROL GROUP, WHICH WAS THE UNIVERSAL OPT IN, CHOSE 92% OF THE TIME.
VERY SIGNIFICANT.
AND THOSE IN THE ACTIVE CHOICE CONDITION, WHICH IS LARGELY THE STRUCTURE THAT'S ENCOURAGED BY GDPR PARTICIPANTS LOGGED IN AROUND 11 AND A HALF % LESS OR 80% OF THE TIME.
SO THIS DEFINITELY HAD AN EFFECT, NOT TOO DRASTIC OF AN EFFECT BUT VERY SIGNIFICANT.
AND LAST IMPRESSIVELY THE PROTECTIVE OPT-OUT MANIPULATION PRODUCED A 41 DECREASE IN LOG IN RATES, WITH THOSE PARTICIPANTS LOGGING IN ONLY ABOUT HALF OF THE TIME.
SO YOU CAN KIND OF SEE THE DIFFERENT TIERS OF PROTECTIVE OF THE DIFFERENT ARCHITECTURE STRUCTURES, SOMETHING THAT YOU

KNOW, WE CAN USE GOING FORWARD TO FURTHER KIND OF FIND A PROPER BALANCE FOR PRIVACY REGULATION.
WE GO TO THE NEXT SLIDE, PLEASE.
SO PERHAPS OUR MOST INTERESTING RESULTS CAME FROM THE CONSIDERATION OF REVERSIBLE CONSENT.
WE FOUND THAT WHEN PAIRED WITH A PROTECTIVE OPT-OUT BOTH REVERSE ABILITY AND ERIE REVERSE ABILITY HAD STRONG NEGATIVE EFFECTS ON LOGGING IN, THIS WAS INCREDIBLY SURPRISING TO US, GIVEN THAT SEEMINGLY OPPOSITE CONSTRUCTS REVERSE ABILITY AND ERIE REVERSE ABILITY HAD THE SAME DIRECTIONAL EFFECTS WHAT THIS TELLS US IS DESPITE INITIAL THOUGHT THAT REVERSE ABILITY TO MAY MAKE INDIVIDUALS MORE LACKS AND LEAD TO HIGHER RATES CONSENT GIVING THE USER INFORMATION AT ALL IS A SIGNAL OF THE SERIOUSNESS OF THE DECISION, THIS IN ESSENCE SCARES THEM OUT OF CONSENTING.
SIMILARLY THIS AFFECTED ONLY FOUND WHEN PAIRED WITH AN OPT-OUT, THIS TELLS US THAT USER ALSO RECOGNIZE THAT WHEN PRESENT WANTED ANY PRIVACY PROTECTIVE CHOICE ARCHITECTURE IT'S LIKELY DUE TO SOME SENSITIVITY REGARDING DECISION, THESE TWO EFFECTS INTERACT STRONGLY TO INFLUENCE THE LOG IN DECISION.
SO FINALLY WE LOOK AT THE EFFECTS OF REPETITION ACROSS THREE ITERATIONS.
WE CAN SEE THE EFFECTIVE IS DEPENDANT ON REVERSE ABILITY TO, WITHOUT ANY INFORMATION ON REVERSE ABILITY THOSE IN THE CONDITION THAT RECEIVED NO

STATEMENT, EFFECT OF OPT IN
DEFAULT GETS STRONGER OVER TIME.
YOU CAN SEE THE OWE EFFICIENCY
FOR THE CONSTANT VARIABLE THINK
ABOUT THAT AS THE AVERAGE OF
THOSE THAT LOGGED IN IN THE
UNIVERSAL OPT IN.
YOU CAN SEE STUDY ONE SAW 92% OF
PARTICIPANTS LOGGING IN BY THE
FINAL EXPOSURE UP TO ALMOST 96%
LOGGING IN, THIS IS KIND OF THE
WORST CASE SCENARIO IN WHICH A
-- A CHOICE ARCHITECTURE THAT
REALLY TAKES AHOLD OF PEOPLE'S
COGNITIVE BY SEES NOT ONLY HAS A
VERY SIGNIFICANT EFFECT UP FRONT
BUT CONTINUES TO GET STRONGER
OVER TIME.
AND HOWEVER, WHEN THEY'RE GIVEN
AN OPT IN STRUCTURE AND ARE
GIVEN INFORMATION ON REVERSE
ABILITY, THE EFFECT OF THE
DEFAULT IS STILL STRONG WITHOUT
A DOUBT BUT REMAINS CONSTANT
OVER TIME THE LAST THREE COLUMNS
YOU CAN SEE THAT YOU KNOW, IT'S
SIMILARLY STARTS AROUND 92% AND
THAT REMAINS CONSTANT ACROSS THE
ITERATIONS OF THE STUDY.
THIS TELLS US THAT REVERSE
ABILITY AND IRREVERSE ABILITY
COUNTERACTS THE GROWTH OF
DEFAULT WE'VE SEEN OTHERWISE AND
A SIMILAR PATTERN FOR OPT OUT
WHERE IT GROWS STRONGER OVER
TIME AND ABSENCE OF REVERSE
ABILITY, BUT WHEN REVERSE
ABILITY IS INTRODUCED THE
EFFECTS ARE KIND OF ALL
PUBLISHED TO THE FOREFRONT WHERE
THERE'S KIND OF A STRONGER
INITIAL IMPACT OF OPT-OUTS BUT
THAT REMAINS CONSTANT OVER TIME.
SO IF WE COULD GO NEXT SLIDE.

SO YOU KNOW, BASICALLY, WE HAVE
TO ASK WHAT WE CAN TAKE FROM
THESE RESULTS.
AND LARGELY, WHAT WE CONCLUDE IS
THERE'S A DELICATE BALANCE
BETWEEN PROTECTIVENESS AND
ECONOMIC BENEFIT.
SO INDIVIDUALLY EACH CHAIN WE
ENACTED HAD THE DESIRED EFFECT
OF CONSUMERS CHOOSING OPTION
THAT IS MAY BETTER REFLECT THEIR
PRIVACY CONCERNS.
FOR EXAMPLE, ON ACTIVE CHOICE
STRUCTURE, DECREASED LOG INS
ALLOWED FOR INDIVIDUALS TO
EXPLICITLY CHOOSE WHICH OPTION
THEY FELT MOST COMFORTABLE WITH.
ADDITIONALLY INFORMING USER AS
TO THE REVERSE ABILITY OF THE
CHOICE CAN COUNTERACT THE GROWTH
OF DEFAULT EFFECTS OVER TIME.
WHICH IS VERY DESIRABLE.
HOWEVER, INTERACTIVE EFFECTS
HAVE THE ABILITY TO PRODUCE VERY
LARGE SWINGS IN CONSUMER
OUTCOMES.
SO FOR EXAMPLE, LIKE WE HAD SAID
ON THE EFFECT OF REVERSE ABILITY
WAS PAIRED WITH A PROTECT TASK
FORCE OPT OUT.
THAT DROVE CONSENT MUCH FURTHER
DOWN THAN WE HAD ORIGINALLY
ANTICIPATED.
SO THESE FINDINGS PROVIDE VERY
SPECIFIC INSIGHT TO POLICY
LEADERS.
SO WE DON'T GIVE ANSWERS
RELATING TO THE BROAD EFFECTS OF
PRIVACY POLICY, BUT WHAT WE DO
IS ISOLATE SPECIFIC CHANGES AND
PROVIDE BETTER UNDERSTANDING AS
TO THEIR EFFECTS AS WELL AS HOW
THEY INTERACT WITH OTHER
CHANGES.

THIS ALLOWS FOR A MUCH RICHER CONVERSATION AROUND FUTURE REGULATION, AND IS ESSENTIAL IN STRIKING THAT IMPORTANT BALANCE BETWEEN PRIVACY AND ECONOMIC BENEFITS.
SO WITH THAT, I THANK YOU FOR LISTENING.
>> THANKS, CAMERON.
I WANT TO START BY ASKING YOU YOUR STUDY CONSIDERS THE INITIAL CHOICE TO CONSENT OR NOT CONSENT TO TRACKING.
AND MAYBE YOU COULD TALK MORE ABOUT WHAT DOWNSTREAM EFFECTS THIS MAY HAVE ON SUBSEQUENT BEHAVIOR, SUCH AS DISCLOSURE?
>> YES.
ABSOLUTELY.
THANK YOU FOR THAT QUESTION.
SO YOU KNOW, AS I HAD SAID THE STRUCTURE OF THIS EXPERIMENT WAS FIRST THE CONSENT DECISION AND THEN SUBSEQUENT DISCLOSURES.
WE DID SEE SOME SLIGHT INCREASES IN DISCLOSURE.
DIFFERING BY CHOICE ARCHITECTURES, FOR EXAMPLE, THOSE IN THE PROTECTIVE OPT-OUT DEFAULT CONDITIONS DISCLOSE SLIGHTLY MORE THAN THOSE IN THE UNIVERSAL OPT IN HOWEVER VERY SMALL AND NOT STATISTICALLY SIGNIFICANT.
IT COULD BE CONCERNING.
WE WOULD EXPECT THAT MAYBE MORE LACKS PRIVACY SETTINGS WOULD RESULT IN MORE TREPIDATION AROUND DISCLOSING SENSITIVE INFORMATION, WE DON'T HAVE THE INFORMATION TO SUPPORT THAT.
NOW, WE WANT BEING SAID, YOU KNOW, WENT SEE EFFECTS RELATE INNED IN THE ARCHITECTURE BUT WE

DID SEE SOME INTERESTING EFFECTS
RELATING TO REVERSE ABILITY SO
PARTICIPANTS IN A CONDITION
WHERE THE DECISION WAS
EXPLICITLY REVERSIBLE DID
DISCLOSE ALMOST 20% MORE THAN
THOSE THAT WERE GIVEN NO
INFORMATION ABOUT REVERSE
ABILITY.
SO THIS COULD TELL US THAT
CHANGES LIKE ARTICLE SEVEN OF
GDPR THAT REQUIRE REVERSE
ABILITY COULD LOWER CONSENT
RATES BUT THAT MAY HAVE IMPACT
IN INCREASING DISCLOSURE
DOWNSTREAM.
SO THAT'S DEFINITELY SOMETHING
THAT NEEDS TO BE CONSIDERED WHEN
CRAFTING THESE POLICIES.
>> I'D ALSO HOPING YOU MAY BE
ABLE TO TALK ABOUT THE FUTURE OF
YOUR RESEARCH STREAM AND HOW YOU
SEE PRIVACY POLICY EVOLVING.
>> YES.
ABSOLUTELY.
YOU KNOW, SO THAT'S VERY
IMPORTANT AND ALSO VERY BROAD
QUESTION.
SO FIRST AND FOREMOST, I TRULY
DO HOPE THAT YOU KNOW MORE
RESEARCH IS PRODUCED THAT
FOCUSES ON MORE THAN A PUT FEW
ASPECTS, A POTENTIAL FOR NEW
EXCITING IN SIGHTS TO ARISE, THE
HUGE AMOUNT OF CHANGES WE'VE
SEEN IN THE LAST DECADE IS VERY
EXCITING.
BUT IN TERMS OF FUTURE OF
PRIVACY POLICY GENERALLY I THINK
ONE CHANGE WE NEED TO SEE IS A
RE FOCUSING TO THE INDIVIDUAL.
SO WE'VE MADE SOME VERY
IMPORTANT STRIDES IN INSURING
THAT COMPANIES ARE BEHAVING

RESPONSIBLY AND THAT CONSUMERS
HAVE THE TOOLS TO MAKE
RESPONSIBLE DECISIONS.
AT THE END OF THE DAY THE
INDIVIDUAL REMAINS DECISION
MAKER SOCIETY ADDRESSED ISSUES
IN LAST FEW YEARS I THINK
PRIVACY CAN BENEFIT FROM BEING
ONE OF THOSE NEXT CHANGES I'D
LOVE TO SEE THE PRIVACY CONCERNS
DISCUSSED IN THE PANEL TODAY AND
OTHER PANELS KIND OF BECOME
GENERAL KNOWLEDGE AMONG THE
POPULATION, YOU KNOW, AND
WITHOUT THAT POLICY, WELL,
INCREDIBLY IMPORTANT CAN ONLY
GET US SO FAR.
>> ALSO I WANTED -- THAT KIND OF
TIES TO MY NEXT QUESTION, WHICH
IS YOU KNOW, THERE'S BEEN AN
ABUNDANCE STREAM OF RESEARCH
SURROUNDING EFFECTS OF GDPR AND
OTHER REGULATION, BUT MAYBE YOU
CAN TALK ABOUT WHAT HOW YOU SEE
YOUR RESEARCH AND WHERE IT
SPECIFICALLY CONTRIBUTES TO
THESE DISCUSSIONS IN TERMS OF
DISCUSSIONS ABOUT PRIVACY
POLICIES AND RESEARCH OF THEM.
>> ABSOLUTELY.
YOU KNOW, I THINK THAT LARGELY,
A LOT OF THE RESEARCH POLICIES
IN TWO POOLS, A FREE MARKET
ADVOCATE AND TRUST CONSUMERS TO
MAKE THEIR OWN DECISIONS OR YO?
TO PROTECT CONSUMERS, BOTH POOLS
PRODUCED GROUND BREAKING
FINDINGS, INFORMED THE
DISCUSSION AROUND DATA PRIVACY
CONSIDERABLY.
BUT WHAT WE TRY TO DO
DIFFERENTLY WAS KIND OF REMOVE
ANY PREEXISTING IDEA OF HOW
PRIVACY SHOULD BE HANDLED.

WE LOOK SPECIFICALLY AT WHAT HAS CHANGED AND HOW IT IMPACTS CONSUMER DECISION MAKING.
AND OUR RESULTS KIND OF REFLECT THIS APPROACH.
WE SHOW THAT IT DOESN'T HAVE TO BE ONE SIDE OR THE OTHER.
THERE CAN BE A BALANCE BETWEEN THE MARKET AND REGULATION.
AND IMPORTANTLY, POLICY ALSO DOESN'T HAVE TO BE ONE SIZE FITS ALL THE FTC SHOWN US SECTOR AND MEDIUM SPECIFIC REGULATION CAN WORK, FOR EXAMPLE, MAYBE HEALTHCARE PRIVACY NEEDS TO LEAN MORE ON PROTECTIVE SIDE AND ENCOURAGE LOWER RATES OF CONCERTS THROUGH THESE DIFFERENT CHOICE ARCHITECTURES BUT THERE MAY BE OTHER REALMS, BROWSING DATA ONLINE THAT YOU KNOW, MIGHT BENEFIT FROM LETTING THE MARKET TAKE MORE OF A ROLE.
YOU KNOW, THIS IS THE CONVERSATION THAT YOU KNOW, I'M HOPING TO START AND HOPEFULLY THAT FUTURE RESEARCH CAN CONTINUE.
>> I SHARE FURTHER MANY RESEARCH BECAUSE THESE ARE IMPORTANT ISSUES.
I THINK AS NICO STARTED US OUT BY SAYING THEY MAY BE ISSUES AS PEOPLE VIEW AS HAVING BEEN RESEARCHED EXTENSIVELY IN THE PAST THERE IS A LOT THROAFT EXPLORES AS ALL OF YOU HAVE BEEN ADDRESSING IN YOUR PAPERS.
I'M EXCITED TO SEIZE WHERE THESE CONVERSATIONS GO.
SO THANK YOU FOR THAT.
LAST AND CERTAINLY NOT LEAST, I WANT TO TURN IT OVER TO PETER MAYER WHO WILL BE PRESENTING HIS

PAPER.
PETER.
>> YEAH, THANK YOU DANIELLE.
SO MY NAME IS IS PETER MAYER AND I WILL BE PRESENTING THE WORK OF MY COLLEAGUES.
AND THIS IS A OUR INVESTIGATION INTO VIRDZ' AWARENESS, PERCEPTION AND DATA BREACHES THAT ACTUALLY AFFECTED THEM.
NEXT SLIDE PLEASE.
MOST PEOPLE HERE WILL BE FAMILIAR WITH THE TERM DATA BREACH, FOR US DATA BREACH WAS AN EVENT IN WHICH PRIVATE SENSITIVE OR CONFIDENTIAL PERSONAL INFORMATION IS LEAKED TO UNAUTHORIZED THE THIRD PARTIES.
SUCH DATA BREACHES CAN CAN EXPOSE TANGIBLE HARM AND EVEN IF THESE EVENTS HAVE NOT OCCURRED YET, INDIVIDUALS MAY EXPERIENCE EMOTIONAL HARMS AS THEY FEEL VULNERABLE OR ANXIOUS ABOUT EXPOSURE OF THIS DATA AND MISUSE IN THE FUTURE.
NEXT PLEASE.
WHEN WE LOOK AT THE NUMBER OF DATA BREACHES AND EXPOSED DSTA RECORDS OVER TIME, WE SEE THAT DATA BREACHES ARE ON THE RISE.
FOR UNITED STATES, WE SEE THAT THERE WERE MORE THAN 1,000 BREACHES EACH YEAR SINCE 2016.
LEADING TO MORE THAN A BILLION EXPOSED RECORDS OVERALL.
YET DESPITE THIS LARGE ENOUGH OF REACHES, RESEARCH SHOWS THAT CONSUMERS RARELY TAKE ACTION.
SO WE WANTED TO HAVE A CLOSER LOOK WITH THE METHODOLOGY THAT WAS DIFFERENT FROM WHAT HAD BEEN DONE BEFORE.

NEXT SLIDE PLEASE.
SO PRIOR WORK PRIMARILY ASKED PARTICIPANTS ABOUT EXPERIENCE WITH BREACHES IN GENERAL OR ASKING THEM TO DESCRIBE INTENDED REACTION HYPE THETD CAL EXAMPLES.
THEREFORE OUR SURVEY HAS GREAT INCREASED ECOLOGICAL VALIDITY WHEN COMPARED TO THIS PRIOR WORK SINCE PARTICIPANTS WERE MORE LIKELY TO RELATE TO THESE BREACHES AND OUR WORK MITIGATES BIAS.
PROVIDED NEEDED RESPONSES.
NEXT SLIDE PLEASE.
TO SEARCH THIS, DATA FROM DATA BREACHES AND ALLOWS VISIT TOORS ENTER THEIR E-MAIL ADDRESS IN THE WEBSITE AND SEE A OLIST OF KNOWN DATA BREACHES TIED TO THAT.
OVERALL 413 PARTICIPANTS WERE RECRUITED OFF THE PROLIFIC PANEL AND WENT THROUGH SURVEY IN THREE STAGES.
IN THE FIRST STAGE WE ASKED PARTICIPANTS TO PROVIDE THEIR MOST COMMONLY USED EMMY ADDRESS, FOLLOWED BY QUESTIONS ABOUT SEVERAL PROPERTIES OF THE E-MAIL ADDRESS SUCH AS ITS FREQUENCY AND PURPOSE OF USE.
IN CASE THE PARTICIPANTS E-MAIL WAS NOT TIED TO ANY BREACHES BUT PARTICIPANTS WERE GIVEN THE OPPORTUNITY TO ENTER ANOTHER E-MAIL ADDRESS WHICH THEY BELIEVE TO BE MORE LIKELY TO BE INVOLVED IN BREACHES.
IN THE SECOND PHASE, OUR PARTICIPANTS THAT WERE AFFECTED BY AT LEAST ONE BREACH REPRESENTED UP TO THREE SPECIFIC

BREACHES FROM THE FULL SET
RETURNED BY CODE.
FOR EACH BREACH THEN WE
COLLECTED DATA RELATING TO OUR
PARTICIPANTS AWARENESS OF THE
INDIVIDUAL BREACH BEFORE THE
STUDY THEIR PERCEPTION OF CAUSES
AND IMPACTS OF BEING IMPACTED,
DID EMOTIONAL REACTIONS AND IF
THEY'VE DONE OR INTEND TO DO
ANYTHING IN RESPONSE.
IN THE END WE COLLECTED THE
PARTICIPANTS DEMOGRAPHICS AND
SHOWED THEM THE COMPLETE LIST OF
KNOWN BREACHES, TO MAKE SURE
THEY WERE AWARE OF THE RISKS AND
IN ADDITION, WE PROVIDED
RESOURCES IN HELPING INDIVIDUALS
TAKING ACTION AND DEALING WITH
THE POTENTIAL AFTERMATH OF THE
INFORMATION WE SHOWED THEM.
NEXT SLIDE PLEASE.
SO USING THE DATA FROM THE
SURVEY WE AIMED TO ANSWER FIVE
QUESTIONS.
NAMELY, THE FACTORS THAT EFFECT
THE THE LIKELIHOOD OF EXPOSURE
TO DATA BREACHES, THE
PARTICIPANT'S CAN PERCEPTION OF
CAUSES OF DATA BREACHES, THEIR
AWARENESS OF THE DATA BREACHES,
THEIR EMOTIONAL REACTIONS AND
THE RESPONSES TO THE DATA
BREACHES.
IN THIS TALK I WILL ONLY PRESENT
RESULTS REGARDING FOUR OF THESE
RESEARCH QUESTIONS, NAMELY,
QUESTION 1, 3, 4 AND 5.
SO WHAT DID WE FIND?
WILLIAM, IN WHICH SLIDE -- WELL,
NEXT SLIDE PLEASE.
FOR THE FIRST RESEARCH QUESTION
WE INVESTIGATED THE FACTORS THAT
INFLUENCED OUR LIKELIHOOD OF

EXPOSURE AND WE DOWNED THAT MANY PARTICIPANTS WERE ENACTED.
SPECIFICALLY, 73% OF PARTICIPANTS APPEARED IN ONE OR MORE BREACHES.
WITH AN AVERAGE OF 5.4 BLEACHES PER PARTICIPANT.
BEFORE IT BECOMES IMMEDIATELY CURRENT THAT MOST SEEM TO BE AFFECTED BY DATA BREACHES.
NOW USING SOME REGRESSION WE FOUND THAT THE FLUX OF BREACHES ASSOCIATED BY AN E-MAIL ADDRESS INCREASES 8% FOR YEAR OF USE.
WHILE 8% MIGHT SOUND LIKE A RATHER SMALL NUMBER, THE FIGURE ON THE RIGHT SHOWS HOW THIS BUILDS UP OVER TIME.
NEXT SLIDE.
REGARDING AWARENESS, WE FOUND THAT PARTICIPANTS WERE UNAWARE OF THE MAJORITY.
NAMELY, 74% OF THE BREACHES BASED ON THIS SURVEY AND THEY WERE AWARE OF ONLY 80 OF% OF THEM.
NEXT SLIDE PLEASE.
IN RESEARCH QUESTION 4 WE FOUND THAT PARTICIPANTS LIKE RESPONSES SHOW A LOW CONCERN FOR THE BREACHES OVERALL, AS THE MEDIAN WAS ONLY SOMEWHAT CONCERNED.
THIS SENTIMENT WAS ALSO REFLECTED IN THE QUALITATIVE DATA WE COLLECTED AS ILLUSTRATE ID WITH THE CODE NUMBER RIGHT HERE.
NOW THESE TWO ASPECTS THE LOW VARIANCE AND THE LONG CONCERN ARE ACTUALLY QUITE CRITICAL.
NEXT SLIDE.
BECAUSE IN THE INVESTIGATION PERTAINING TO RESEARCH QUESTION 5 WE FOUND THAT BOTH AWARENESS

AND CONCERN ARE KEY PREDICTORS
OF CONSUMERS TAKING ACTION IN
RESPONSE TO A BREACH.
SO TO SUM THIS UP WE FOUND THAT
MOST CONSUMERS SEEMED TO BE
AFFECTED BY DATA BREACHES BUT
ARE LARGELY UNAWARE AND
UNCONCERNED OF IMREECHES THAT
AFFECT THEM.
-- OF BREACHES THAT AFFECT THEM.
THIS IN TURN LEADS TO CONCERN
AFTER BREACH.
SO WHAT ARE THE IMPLICATIONS?
NEXT SLIDE PLEASE.
THAT 74% OF THE BREECHES WERE
UNKNOWN TO PARTICIPANTS, MAY NOT
BE EFFECTIVE.
THEREFORE WE ARGUE THAT IN
IMPORTANT ASPECT OF THE
ADDRESSING THIS ISSUE IS THE
NEED FOR REGULATORS TO PUSH FOR
STRICTER REQUIREMENTS TO REACH
ORGANIZATIONS REGARDING WHEN AND
HOW.
NEXT PLEASE.
IDEALLY, NOTIFICATION CAN BE
DELIVERED IN MULTIPLE CHANNELS
SUCH AS A WRITTEN LETTER AND
E-MAIL OR WHEN A CUSTOMER
ACTUALLY CALLS.
>> TO A COMPANY, THIS COULD ALSO
BE AN OPPORTUNITY TO MAKE THAT
CUSTOMER AWARE AND INFORMED
ABOUT MITIGATING ACTIONS.
USING ALL THESE CHANNELS ALLOWS
INCREASING THE CHANCE OF
REACHING THE AFFECTED
INDIVIDUAL.
BUT THE NOTIFICATION MUST ALSO
BE UNDERSTANDABLE AND USABLE FOR
EVERYONE.
FOR EXAMPLE, THIS COULD BE MADE
BETTER BY INCLUDING EASY TO
ENACT MITIGATION.

THE IMPORTANT BOTTOM LINE HERE
IS THAT REQUIRING BREACH
NOTIFICATIONS IS NOT SUFFICIENT
TO REACH CONSUMERS.
IT ALSO LET US HOW THE
INFORMATION IS PROVIDED TO MAKE
SURE PEOPLE REALLY PAY
ATTENTION, UNDERSTAND THE RISKS
AND ARE MOTIVATED TO TAKE
PROTECTIVE ACTION.
SO THE QUESTION IS WHAT TO DO
ABOUT IT.
NEXT SLIDE PLEASE.
AND HERE WE ARGUE THAT
NOTIFICATION ALONE IS NOT
ENOUGH.
AND COMPANIES SHOULD BE REQUIRED
TO STAY INVOLVED IN HELPING
AFFECTED INDIVIDUALS RECOVER
FROM DATA BREACHES RATHER THAN
PROVIDING FREE CREDIT OR
IDENTITY MONITORING SERVICES
WHICH HAVE LIMITED PREVENTIVE
PROTECTIONS REGULATORS SHOULD
ENCOURAGE COMPANIES TO OFFER
MORE PROTECTION TOOLS.
ONE EXAMPLE HERE, IS TOOLS THAT
ALLOW CREATING UNIQUE E-MAIL
ALIASES DURING THE PHASE.
NEXT PAGE PLEASE.
FOR EXAMPLE SIGN IN WITH APPLE
PLOWS USERS TO PROVIDE AN E-MAIL
ADDRESS BUT THEY CAN ALSO CHOOSE
TO HIDE THAT E-MAIL WHICH MEANS
E-MAIL ADDRESS FOR THE SIGN IN
AND FORWARD THE INCOMING
PARTICIPANTS, ASSIGNING WITH
APPLE AND SIMILAR TOOLS SEE MORE
WIDESPREAD DEPLOYMENT.
MORE RESEARCH IS NEEDED TO
UNDERSTAND MOTIVATORS AND
BARRIERS BEHIND ADOPTION OF SUCH
TOOLS.
BUT OFFERING THESE TOOLS IN A

WELL INTEGRATED WAY WOULD ENABLE
USERS TO PROTECT THE DATA WITH
BASICALLY NO ADDITIONAL FRICTION
IN THE PROCESS AND ADDITIONALLY,
HAVING THESE UNIQUE E-MAIL
ADDRESSES WOULD ALLOW USERS TO
IDENTIFY WHICH SERVICES HAVE
LEAKED OR SOLD THEIR DATA, IN
CASE THEY APPEAR IN SPAM OR
FIRVING E-MAILS.
ABOUT NEXT SLIDE PLEASE.
INTEGRATED INTO POSITIVE
MANAGEMENT SUCH AS FIREFOX LOCK
WISE WHICH YOU CAN SEE ON THE
RIGHT HERE, LET USERS LEARN
ABOUT BREACHES AND TAKE
AVAILABLE ACTION IN THE MOMENT
AS THEY VISIT A BREACHED SITE OR
ASSERT THEIR CREDENTIALS.
AND SO BOTH OF THESE
TECHNOLOGIES I JUST MENTIONED
CAN MORE FUNDAMENTALLY HELP
CONSUMERS FINISH THEIR ONLINE
PRESENCE AND STAY SECURE BY
OFFERING BENEFITS BEYOND THE
CONTEXT OF DATA BREACHES IN THE
SLIDE HERE.
NEXT SLIDE.
AND THIS BRINGS ME TO THE END OF
MY TALK.
THIS RESEARCH WAS DONE BY MY
COLLEAGUES, AN MYSELF AND IF YOU
WANT TO CHICK OUT THE FULL PAPER
YOU CAN FIND LINK ON THE QR CODE
ON THIS SLIDE.
AND THANK YOU VERY MUCH.
>> THANK YOU PETER.
I WANTED TO -- THIS IS
FASCINATING AND IT'S REALLY
INTEREST BEING TO HEAR ABOUT
YOUR VIEWS -- INTERESTING TO
HEAR YOUR VIEWS AND RESEARCH ON
CONSUMERS AWARENESS OR LACK
THEREOF OF THE MANY BREACHES

THAT AT LEAST THE CONSUMERS IN
YOUR STUDY WERE AFFECTED BY AND
THEN IF RULES THAT EVERYONE CAN
PLAY TO HELP THEM.
AND TO MITIGATE THE EFFECTS.
I WANTED TO START BY ASKING YOU,
ABOUT WHAT CONSUMERS CAN DO TO
PROTECT THEMSELVES AND TO
MITIGATE THE EFFECTS OF DATA
BREACHES.
AND ALSO, WHAT CONSUMERS CAN DO
IN RESPONSE, WHEN THEY DO FIND
THEMSELVES TO BE AFFECTED BY A
BREACH.
>> SO THE MOST EFFECTIVE WAYS TO
MITIGATED EFFECT IS PROACTIVE
MEASURES.
SO BEING PROACTIVE, WHEN
CREATING ACCOUNTS, MAKING A
CONSCIOUS DECISION ABOUT WHETHER
I -- WHETHER I NEED THE ACCOUNT,
AND WHICH DATA I ACTUALLY HAVE
TO PROVIDE TO CREATE THIS.
AND TO PROTECT THE DATA THAT IS
ACTUALLY NEEDED TO CREATE AN
ACCOUNT, WE HAVE SEEN THAT THERE
ARE PROACTIVE MEASURES SUCH AS
THE E-MAIL ALIASES AND THERE ARE
SEVERAL TECHNOLOGIES AVAILABLE,
INTEGRATED OPTIONS LIKE SIGNING
IN WITH APPLE WORK GREAT DID YOU
ACTUALLY HAVE AN APPLE DEVICE.
BUT THERE ARE OTHER PLAYERS IN
THIS MARKET.
MOZILLA HAS A SIMILAR SERVICE
AND THERE ARE OTHERS.
SO USING THOSE PROACTIVE
MEASURES IS ONE OF THE BEST
CHOICES WHEN YOU ACTUALLY HAVE
TO PROVIDE DATA.
AND THEN AS RESPONSES TO A
BREACH, THE MOST IMPORTANT THICK
IS TO FIRST SEE WHICH DATA IS
DEVELOPMENTALLY AFFECTED.

BECAUSE THE RESPONSE DEPENDS ON WHICH DATA AHAS ACTUALLY LEAKED.
FOR EXAMPLE, IF THE PASSWORDS OR IF A PASSWORD IS LEAKED, YOU SHOULD CHANGE THAT PASSWORD AS SOON AS POSSIBLE.
AS SOON AS YOU BECOME AWARE OF THAT BREACH.
BUT ALSO, IF THAT PASSWORD WAS USED ON DIFFERENT WEBSITES, YOU SHOULD CHANGE IT THERE AS WELL.
BECAUSE THERE ARE ATTACKS THAT JUST REUSE WHAT HAS BEEN USED ON THE WEBSITE SO IT'S IMPORTANT NOT TO VIEW THIS SERVICE IN ISOLATION BUT SEE WHERE IT MIGHT CAUSE OTHER PROBLEMS.
AND THIS MIGHT ACTUALLY BE A GOOD CHANCE, YOU KNOW, IF YOU ARE CREATING A NEW PASSWORD ANYWAY, TO ADOPT THE DIFFERENT STRATEGY OMANAGE YOUR ONLINE PRESENCE FOR EXAMPLE, PASSWORD MANAGER, FOR EXAMPLE, WITH THESE BUILT IN NOTIFICATION OPTIONS, THAT AUTHENTIC HELPS YOU TO -- THAT THEN HELPS YOU STAY ON TOP OOF THINGS EVEN MORE.
>> THANK YOU.
THOSE ARE ALL REALLY HELPFUL SUGGESTIONS.
I WANTED TO THEN TURN TO THE ACTIONS THAT ORGANIZATIONS CAN TAKE TO MITIGATE THE EFFECTS OF BREACHES.
I MEAN THERE ARE SO MANY DIFFERENT LAYERS IN THIS ECOSPHERE OF DIFFERENT ENTITIES THAT YOU KNOW CONSUMERS WILL INTERACT WITH.
BUT SPECIFICALLY WHAT DID YOUR RESEARCH SHOW IN TERMS OF BREACHED ORGANIZATIONS, WHAT SORT OF EFFECTS CAN -- OR WHAT

ACTIONS CAN THEY TAKE TO BEST MITIGATE THE EFFECTS OF THE BREACHES THAT THEY'VE ENCOUNTERED FOR CONSUMERS?
>> I THINK THE BIGGEST FACTOR THAT WE IDENTIFIED HERE THAT IS RELEVANT FOR THIS QUESTION IS THE LACK OF WAGES THAT WE SAW -- AWARENESS THAT WE SAW IN OUR PARTICIPANT SAMPLE.
AND THIS INDICATES THAT COMPANIES REALLY NEED TO BE MORE ACTIVE WHEN NOTIFYING THEIR CONSUMERS.
BECAUSE BEFORE I CAN ACT, TAKE PROTECTIVE ACTIONS, I NEED TO BE AWARE THAT SOMETHING HAS HAPPENED.
AND SO COMPANIES SHOULD NOTIFY THEIR CUSTOMERS AS SOON AS THE COMPANY BECOMES AWARE OF THE BREACH.
AND WELL TO BECOME AWARE THEY SHOULD HAVE A MONITORING OF THEIR ASSISTANCE TO SEE IF SOMETHING GETS LOST.
IF SOMETHING ACTUALLY HAPPENS THEN THEY SHOULD USE EVERY CHANNEL THEY HAVE AT THEIR DISPOSAL, RIGHT?
THE TRADITIONAL WAYS HAVE PROVEN TO BE NOT TOO EFFECTIVE AND SO INTERACTING WITH THE CUSTOMERS ON THAT PARTICULAR BREACH LIKE IF THEY CALL IN TO ORDER SOMETHING AND YOU KNOW THAT THEY HAVE NOT CHANGED THEIR PASSWORD YET THIS MIGHT BE A PERFECT OPPORTUNITY TO CALL THEM ON IT.
AND TO REALLY GO OUT THERE LIKE IT MIGHT NOT BE REALLY FOR THE COMPANY A DESIRABLE THING TO HAVE A BIG BANNER ON THEIR SPHROONT PAGE THAT SAYS YOU KNOW

WE HAVE BEEN AFFECTED BUY DATA BREACH.
BUT IT WOULD DEFINITELY HELP MAKE PEOPLE AWARE.
AND SO COMPANIES SHOULD BE MORE OPEN TO TAKE CREATIVE APPROACHES, TO NOTIFYING PEOPLE.
AND NOW FOR ORGANIZATIONS IN TERMS OF DEVELOPERS, THEY MIGHT ALSO WANT TO INTEGRATE THESE TECHNOLOGIES INTO THEIR TOOLS, FOR EXAMPLE, ALLOW SIGN-IN WITH -- SIGN-IN WITH APPLE OR SIMILAR TECHNOLOGIES, SUPPORTth IN THE APP SO THAT CONSUMERS CAN ACTUALLY CHOOSE THIS TECHNOLOGY.
AND I THINK FOR LIKE WE WOULD LIKE ORGANIZATIONS TO BE MORE PROACTIVE AND REALLY NOTIFY ABOUT ALL THE BREACHES, NOT JUST HIGH-RISK ONES, THAT IT HAS ACTUALLY BEEN SHOWN AND THIS IS NOT OUR RESEARCH BUT RELATED RESEARCH THAT COMPANIES THAT TAKE RESPONSIBILITY AND THAT HELP PEOPLE IN THIS SITUATION, ACTUALLY FACE LESS SEVERE CONSEQUENCES IN TERMS OF LOSSES, FOR EXAMPLE.
>> THANK YOU.
THEN FINALLY, I WANTED TO ASK YOU, WE'VE NOW TALKED TO CONSUMERS AND ORGANIZATIONS, BUT FROM A REGULATORY STANDPOINT, WHAT DOES YOUR RESEARCH SUGGEST ABOUT FUTURE REGULATIONS FOR DATA BREACHES?
AND WHAT IS WHAT YOU FOUND OR FOUND TO BE EFFECTIVE OR FOUND NOT TO BE EFFECTIVE?
>> SO I THINK THE MOST IMPORTANT THING IS THAT ORGANIZATIONS NEED TO BE NUDGED, IF NOT MORE

PROACTIVE, NOT JUST WITH HIGH RISK ONES BUT ALSO WITH ANY BREACH THAT OCCURS.
BECAUSE IT HAS BEEN SHOWN THAT, IT'S OFTEN UNCLEAR HOW HIGH RISK A BREACH ACTUALLY IS.
SO IT MAKES SENSE TO JUST NOTIFY CUSTOMERS WHENEVER THERE IS A BREACH.
AND OVERALL GETS ORGANIZATIONS TO TAKE MORE RESPONSIBILITY THERE AND TAKE CREATIVE APPROACHES TO HELP RAISE AWARENESS ABOUT THE BREACHES THAT OCCUR.
>> THANK YOU PETER.
AND I WANTED TO THANK ALL OF OUR PANELISTS.
PETER, CAMERON, NICO AND SIDDHANT TODAY FOR PRESENTING THIS RESEARCH.
I THINK IT'S ALL VERY INTERESTING AND NOVEL RESEARCH ON THIS ISSUE OF PRIVACY NOTION AND DATA BREACHES WHICH, YOU KNOW, WELL HAS BEEN ADDRESSED BEFORE THESE ARE NEW AND DIFFERENT AND INNOVATIVE WAYS TO EXPLORE THEM AND HOPEFULLY WILL BE SOMETHING THAT YOU AND OTHERS BUILD ON IN THE FUTURE.
[LUNCH RECESS]
.
.
.
.
WE WILL LEARN ABOUT VERY INTERESTING RESEARCH BEING CONDUCTED ON PRIVACY.
MY NAME LINDA HOLLERAN I'M AN ATTORNEY WITH THE FTC DIVISION OF PRIVACY AND IDENTITY PROTECTION.
PANEL WILL FIRST DISCUSS

RESEARCH RELATED TO PRIVACY COMPLIANCE OF APS USED WITH VOICE PERSONAL ASSISTANCE LIKE ALEXA OR GOOGLE HOME THAT SO MANY OF US HAVE.
WE WILL LOOK AT PRIVACY ON IMT DEVICES CAN IMPACT RECEPTION OF THE PRIVACY RISK OF USING DEVICE AS WELL AS THE WILLINGNESS TO PURCHASE THE PRODUCT.
A FINAL PRESENT ER WILL TALK ABOUT AN INTERESTING NEW DYNAMIC TOOL DESIGNED TO TALK ABOUT A REAL-TIME PROVES ANALYSIS OF IOT APS.
AT THE END WE'LL HAVE AN OPPORTUNITY FOR QUESTIONS AND ANSWERS, IF YOU HAVE ANY QUESTIONS PLEASE E-MAIL THEM TO PRIVACY CON AT FTC.GOV AND WE'LL TRY TO GET TO THEM AS TIME PERMITS.
LET'S GET STARTED.
FIRST WE'LL HEAR IF ANUPAM DAS AT NC STATE UNIVERSITY, PRESENT HIS PAPER, ANY ALEXA IS THIS SKILL SAFE, TAKING A CLOSER LOOK AT THE ALEXA SKILL ECOSYSTEM.
>> THANK YOU, LINDA FOR THE NICE INTRODUCTION.
TODAY, I'M GOING TO TALK ABOUT OUR RECENT WORK INCLUDE IDENTIFYING SOME PROCESS FOR THIRD PARTY APPLICATION OF THE ALEXA SYSTEM.
LET'S SEE WHAT ALEXA IS AMAZON SMART VOICE ASSISTANT AND THERE ARE MULTIPLE VENDORS OUT THERE AND STATISTICS SAY THERE'S ALMOST 4 BILLION ACTIVE DEVICES.
PANE OF THES THINGS DRIVING THE ADOPTION IS LOT OF THE SMART DEVICES ARE COMING OUT OF THE MARKET RIGHT NOW ARE, CAN EASILY

INTEGRATE WITH VOICE ASSISTANT
WHICH MEANS USERS CAN EASILY
CONTROL SMART AND DEVICES
THROUGH THE VOICE ASSISTANT.
ANOTHER NEAT FEATURES COMING OUT
FROM A LOT OF THIS.
ASSISTANT PLATFORMS IS A LOT ARE
OPENING UP AND BEING ABLE TO
APPLICATIONS ON TOP OF THE VOICE
ASSISTANT.
SO IN THE CASE OF ALEXA, THIS
THIRD PARTY APPLICATION IS
TYPICALLY KNOWN AS SKILLS.
AND, AND ALL.
ALL YOU NEED TO DO, IN ORDER TO
INSTALL AND INTERACT IS USE
VOICE INTERFACE.
FOR EXAMPLE, IF YOU WANT TO
INSTALL OR INTERACT WITH ONE OF
THE THIRD PARTY SKILLS ALL YOU
NEED TO SAY IS ALEXA OPEN
FOLLOWED BY THE APPLICATION NAME
FOR THE PARTICULAR THIRD PARTY
SKILL IN TH YOU WANT TO INTERACT
WITH.
FROM THE POINT OF VIEW THAT MEAN
YOU CAN ALWAYS, YOU CAN DOUBLE
UP IN THE APPLICATIONS AND
SUBMIT IT FOR TO -- SUBMIT THE
IT FOR OTHER PEOPLE TO USE.
NEXT.
SO IN TERMS OF OUR RESEARCH
QUESTIONS, WE WILL TRYING TO
LOOK AT THIS OVERALL VETTING
PROCESS THAT GOES INTO THIS
ALEXA SKILL SYSTEM, WE'RE
LOOKING AT EXISTING LIMITATIONS
THAT MIGHT BE EXPLOITED BY
ATTACKERS.
ONE OF THE THINGS THAT WE LOOKED
AT IS THAT IN THAT IN FOR THE
ALEXA SYSTEM IS THAT YOU CAN
HAVE APPLICATIONS THAT HAVE
DUPLICATE IMPLICATIONS YOU CAN

HAVE THE DIFFERENT DOUBLE UP SKILL THAT IS HAS SAME IDENTICAL IMPLICATION NAME, THIS CAN CAUSE CONFUSION IN THE SENSE IF A USER WANTS TO ACTIVATE A SKILL THROUGH THE VOICE INTERFACE, USER MIGHT NOT KNOW WHICH PARTICULAR SKILL IS BEING ACTIVATED.
WE LOOKED AT THIS AND WHICH ATTRIBUTES MIGHT BE USED TO KIND OF ACTIVATE A PARTICULAR SKILL.
THEN WE LOOKED UP, ANY SKILLS ON THE, THIS IS IMPORTANT BECAUSE, YOU CAN LAUNCH POTENTIALLY FISHING ATTACKS THROUGH THIS LIMITATION.
ANOTHER THING WE LOOKED AT IS THAT IN THE CONTEXT OF SKILL, IS THAT AMAZON WAS PROPERLY VETTING ALL THE DIFFERENT DATA TYPES, PARTICULAR A PARTICULAR SKILL TRYING TO REQUEST, DIGITALLY CAPTURED THROUGH THE TERM INTENT IN THE CONTEXT OF A SKILL.
ANOTHER THING WE WERE LOOKING AT IS LIKE ANY OTHER PLATFORMS AMAZON ALSO HAS A PERMISSION API THAT CAN THAT IS MADE AVAILABLE TO THIRD PARTY APPLICATIONS AND BUT WE WERE ALSO LOOKING AT WHETHER A LOT OF THE SKILLS WERE BYPASSING THIS PERMISSION MODEL AND ACTUALLY INVOKE, THE SENSITIVE DATA.
NEXT WE LOOK AT AND LOOKING AT LOOKED AT WHETHER YOU CAN ACTUALLY DO ATTACKS IN THIS KIND OF I COMPANY SYSTEMS GIVEN THAT YOU CAN INVOKE THE SKILL THROUGH THE VOICE INTERFACE, IT'S EASIER, WE LOOKED AT WHETHER IT'S PHYSICAL AND IF SO, WHICH WAS MORE PUT EFFECTIVE?

AND LASTLY WE LOOKED AT THE
PRIVACY POLICIES OF A LOT OF THE
SKILLS AND WHETHER THE PRIVACY
POLICIES WERE PROPERLY
DISCLOSING THE DATA TYPES THAT
THE SKILLS WERE REQUESTING.
SO BEFORE I GO INTO THE FINDINGS
AND LET ME BRIEFLY HIGHLIGHT HOW
WE ACTUALLY CONDUCTED THIS WHOLE
ANALYSIS, WE PULLED THE TOP
SEVEN ALEXA SKILLS STORES, FROM
CANNED, U.S., UK GERMAN AND
JAPAN AND OVER 90,000 SKILLS WE
WERE THE ABLE TO IDENTIFY.
AND THEN WE WERE BASICALLY
SCRIPING MET AT A DATA FROM THE
PAGES LIKE THE SKILL NAME.
THE RATINGS IF IT'S A PART OF AS
PRIVACY POLICY, WHAT IS THE
PRIVACY POLICY LINK AND SO ON.
NOW, IN ORDER TO TEST WHICH
PARTICULAR SKILLS MIGHT
ACTIVATE, WE USED A
SEMIAUTOMATIC APPROACH.
WHERE WE USED, AND TO ANALYZE
THE PRIVACY POLICY OF SKILLS WE
USED EXISTING SKILLS LIKE POLY
CHECK WHICH IS A TOOL THAT
ENABLES YOU FIND CONSISTENCY
WITHIN THE PRIVACY POLICIES
THEMSELVES.
AND LASTLY, WE ALSO PUBLISHED
OUR SKILLS TO VALIDATE SOME
FINDINGS.
LET ME GO TO THE FIRST POINTS.
AND SO THE FIRST POINT IS GIVEN
THAT THERE ARE MULTIPLE SKILLS
WITH IDENTICAL INVOCATION NAMES,
THE VERY FIRST QUESTION WAS HOW
DOES AMAZON SELECT WHICH SKILL
TO ACTIVATE AND CAN THIS
ACTIVATION PROCESS LEAD TO
ACTIVATING THE WRONG SKILL?
SO WE TRIED, IDENTIFYING VARIOUS

PUBLIC ATTRIBUTES ASSOCIATED WITH A GIVEN SKILL.
FOR EXAMPLE, IF YOU GO TO SKILLS PAGE YOU CAN LOOK AT THE VARIOUS NUMBER OF RATINGS GIVEN TO THIS SKILL, THE AVERAGE RATING THAT THE SKILL HAS, OR THAT THE SKILL HAS ANY PERMISSION REQUESTS, YOU CAN EVEN IDENTIFY THE DATA OF THE SKILL AND WHETHER THE SKILL HAS LABELS.
WE TRIED TESTING WITH VARIOUS ATTRIBUTES PUBLICALLY AVAILABLE AND THEN WE DID SOME STILL ANALYSIS TO FIND OUT IF ONE OF THE ATTRIBUTES IS STRONGLY CORRELATED IN TERMS OF WHAT IS ACTIVATED AND FOUND THAT SKILLS TYPICALLY THAT HAVE HIGHER RATINGS OR AVERAGE RATINGS HAS A STRONG IN TERMS OF GETTING ACTIVATED.
THAT SHOWS CORRELATION BUT NOT CAUSATION, WE WANT TO TEST THIS OUT.
THIS IS WHERE WE DOUBLE UP OUR OWN SKILL AND PUSH AND PUBLISH THOSE SKILLS AND WANTED TO SEE IF WE CAN MANIPULATE SOME ATTRIBUTES AND SEE IF THE ACTIVATION PROCESS CHANGED.
SO WE ARRANGED TWO DIFFERENT SKILLS, AND WITH THE SAME IDENTICAL INVOCATIONS AND WE CHECKED WITH ONE FIRST TO SEE IF IT WAS PROPERLY ACTIVATED, WAITED A WEEK AND THEN PUNISHED THE NEXT ACCIDENT WITH THE SAME INVOCATION PLACED AND CHECKED WHICH PARTICULAR SKILL WAS ACTIVATED.
TURNED OUT THE NEW SKILL WAS ACTIVATED INSTEAD OF THE OLD ONE.

SO THAT'S KIND OF INDICATES THAT THERE'S A PARTICULAR CHOICE THAT AMAZON MAKES IN TERMS OF WHICH PARTICULAR SKILLS TO ACTIVATE.
STATISTICALLY WE FOUND THAT RATING WAS ONE OF THE INFLUENTIAL FORECAST WE SAY TRIED TO THEN CHECK IF WE CAN INCREASE THE RATING OF THE OLD SKILL TO MANIPULATE THE HOLE SELECTION PROCESS, WE DID THAT BUT UNFORTUNATELY THAT DID NOT RESULT IN THE CHANGE IN THE SELECTION PROCESS.
SO THAT INDICATES THAT AND THAT AMAZON IS PROBABLY USING SOME INTERNAL FEATURES WHICH IS NOT PUBLICALLY AVAILABLE TO SELECT THE SKILLS.
SO THE TAKE AWAY MESSAGE IS THERE ARE DUPLICATE SKILLS WITH THE SAME IDENTICAL INVOCATIONS AND GIVEN THAT ALEXA NOW HAS THE ENABLED FEATURE, WHICH MEANS THAT IF YOU ASK FOR A PARTICULAR -- IF YOU INVOKE ONE OF THE SKILLS AND IF THERE'S A MATCH FOUND IT WILL AUTOMATICALLY INSTALL IT ON YOUR ACCOUNT.
THIS CAN POTENTIALLY LEAD TO ACTIVATING THE WRONG SKILL.
SO THE OTHER -- SO THE -- SO THENQh
INTO IS THE REGISTRATION.
CAN AN ATTACKER PLACE SKILLS UNDER ANY ARBITRARY, WHAT WE DID IS TRIED TO MATCH SKILLS WITH DIFFERENT DOUBLE UP -- IN OUR CASE, WE TRIED TO LIST SKILLS UNDER THE MAIM OF MICROSOFT AND PHILLIPS, A LOT OF TIME WE SUCCEED.
YOU CAN SEE WITH MICROSOFT, AND RING, BUT DID NOT BUT WE DID NOT

UNDERWRITER THE NAME OF FELLOWS.
ONE THING WE FOUND AND THE
REASON FOR THIS COULD BE IS THAT
WHEN YOU SUBMIT A SKILL, THEY'RE
VETTED AND THERE'S AN AUTOMATION
IN THIS PROCESS, WE BELIEVE ONE
CASE THAT WAS NOT SUCCESSFUL
WOULD BE THE CASE WHERE A VET ER
MIGHT HAVE REALIZED THIS IS A
SKILL BEING PUSHED UNDER A
DIFFERENT -- AND THIS COULD BE
THE REASON IT WAS FLAT.
ONE OTHER INTERESTING THING WE
ALSO FOUND IS THAT ONCE IF YOU
DO SUCCEED, FOR EXAMPLE, FOR THE
RINK IF YOU DO SUCCEED AND IF
YOU CLICK THE RATING TAB, HOT
LINKS THE DOUBLE UP PERSON TO
ANY OTHER PRODUCT THAT IS AMAZON
HAS UNDER THAT DOUBLE UP PERSON
NAME.
SO THIS SPECIFICALLY CAN CAUSE
CONFUSION TO CONSUMER THINKING
THAT THIS IS ACTUALLY DOUBLE
UPPED BY THIS RING THE
PARTICULAR MESSAGE IS WE FOUND
IS IT IS POSSIBLE TO LIST SKILL
UNDER WELL-KNOWN COMPANY NAMES.
SO THE -- SO THE NEXT THING THAT
WE ANALYZE IS THE CHANGE OF BACK
AND FORTH.
SO WHEN SAY BACK AND FORTH, THIS
IS IN THE CONTEXT OF A THIRD
PARTY APPLICATION, WHERE THE
THIRD PARTY APPLICATION CAN
CONTROLS THE BACK END OF HOW THE
PROCESS THE DATA AND HOW THEY
WANT TO INTERACT WITH THE USER.
ONE OF THE THINGS THAT HAPPENED
WE TESTED OUT IS THAT SINCE
SKILLS HAVE TO REGISTER FOR THE
PARTICULAR DATA TYPES THAT THEY
WANT TO INTERACT WITH, THAT THEY
WANT TO INTERACT WITH, AND

TYPICALLY THIS TERM -- THE DATA TYPES ARE TERMED INTENT, IS THAT YOU CAN RAISE UP ANY ARE BY AT HER NUMBER OF INTENT, WHETHER THEY'RE ACTIVELY USED OR NOT.
BUT WE LISTED MULTI-AGENTS AND SOME WERE SENSITIVE, FOR EXAMPLE, WE USED A PHONE NUMBER, AND WE THEN BASICALLY TESTED THE SKILL AND VETTED THE SKILL, WHICH SUBSEQUENTLY WE SUBMITTED THE SKILL AND THE SKILL WAS VETTED BUT IT DID NOT TRIGGER ANY OF THE SENSITIVE INTENT TYPES AND IT WAS EVENTUALLY APPROVED, AND WHAT I MEAN APPROVED, IT WAS PUBLICALLY AVAILABLE AT THAT POINT.
SO ONCE THAT WAS PUBLICALLY SABLE.
WHAT WE DID IS WENT TO THE BACK END BECAUSE THIS IS THE BACK END WE CONTROL AS THE DEVELOPER, WE CHANGED INTERACTIVE DIALOGUE, BASICALLY AT THIS POINT, WE'RE ASKING FOR THE PHONE NUMBER WHERE PREVIOUSLY THIS WAS NEVER TRIGGER DURING THE VETTING PROCESS.
SO THIS WHOLE PROCESS MEANS THAT IT ADVERSELY CAN POTENTIALLY IT IS THE INTENT AN DEVELOPER IS RE TRIGGER RETREAT SENSITIVE INFORMATION FROM THE END USERS.
NEXT WE LOOKED AT WHETHER THE SOME OF THE SKILLS WOULD ACTUALLY BYPASS PERMISSION MODEL.
BEFORE I START THAT.
AMAZON DOES -- LET ME EXPLAIN WHAT THE -- AMAZON DOES HAVE PERMISSION API MODEL WHICH ENABLES BASICALLY DEVELOPERS TO SENSITIVE INFORMATION FROM THE

MODEL.
IF YOU DO USE THIS, WHAT MEANS IS ALEXA BASICALLY FORWARDS THE END USERS TO THE AP TO APPROVE OR GIVE CONSENT TO USER SENSITIVITY INFORMATION.
THIS IS VOLUNTARILY HAS TO BE DECLARED BY THE DEVELOPERS, SO WE WANTED TO SEE IF THERE WERE SKILLS THAT WERE BYPASSING THIS INFORMATION ON API AND ASKING THE SENSITIVE INFORMATION FOR THE VOICE INTERFACE ITSELF.
WE LOOKED FOR SENSITIVE FOR TODAY TYPES LIKE PHONE NUMBER, LOCATION, E-MAIL AND NAME WE SEARCHED FOR THIS -- THIS TERMS WITHIN SKILL DESCRIPTION PAGE AND SO THIS SKILL DESCRIPTION PAGE IS INFORMATION AVAILABLE PUBLICALLY ON THE WEBSITE AND WE BASICALLY HAD AN OPPORTUNITY TO GO THROUGH THIS AND EXTRACT AND BASICALLY FIND SKILLS THAT WERE ACTUALLY ACCESSING SOME OF THIS.
THIS RESULTED IN US FINDING 350 SKILLS THAT WERE ACTUALLY DESCRIBED USE THEIR DESCRIPTION OF ACCESSING THE SENSITIVE INFORMATIONS, NEXT TASK WAS TO ACTIVATE THE SKILLS TO SEE IF THEY WERE REALLY ACCESSING THE SENSITIVE INFORMATION, THROUGH THE VETTING PROCESS WE FOUND THAT 52 OF THEM WERE ACTUALLY FALSE POSITIVE, WE DIDN'T ASK FOR THAT INFORMATION EVEN THOUGH THE DESCRIPTION PAGE MENTIONED THOSE SENSITIVE INFORMATIONS BUT WE DID FIND 169 SKILLS THAT DID REQUEST THE SENSITIVE INFORMATIONS.
AND SO THAT BASICALLY INDICATES THAT ALEXA MAY NOT BE PROPERLY

MEDIATING THE TYPE BASED ON THE SENSITIVE INFORMATION BEING REQUESTED.
AND SO LASTLY, WE ALSO LOOKED AT THE PRIVACY POLICY, AND SO ONE UNIQUE ATTRIBUTE ABOUT PRIVACY POLICIES WITH ALEXA SYSTEM IS THAT BY DEFAULT SKILLS DON'T NEED TO HAVE A PRIVACY POLICY, THIS IS BIT DIFFERENT FROM GOOGLE ECOSYSTEM, BUT ALEXA DOES MANDATE THE PRIVACY POLICY FOR SKILLS THAT.,0s ACCESS PERMISSION API's, ANY SKILL REQUESTING A PERMISSION DATA TYPE WILL HAVE TO SUBMIT A PRIVACY POLICY LINK OTHERWISE IT WILL NOT APPEAR PUBLICALLY IN SKILL STORE.
SO WE BASICALLY ANALYZED SKILLS THAT WERE ACCESSING THESE TYPES OF PERMISSIONS, AND WE ALSO DOWNLOADED THE PRIVACY POLICIES FOR THE SKILLS AND WE WANTED TO SEE IF THE PRIVACY POLICIES WERE ACCURATELY REFLECTING ON THE DATA TYPES WE WERE CAPTURING, WE ANALYZED 1,124 SKILLS AND FOUND THAT A LOT OF THEM WERE NOT PROPERLY EXPLICITLY ADDRESSING THE SENSITIVE DATA TYPE THEY WERE ACCESSING.
SO IN GENERAL, THE DATA TYPES LIKE FULL NAME, PHONE NUMBER AND LOCATIONS HAD MOST NUMBER OF INCONSISTENCIES IN THE SENSE THEY DID NOT MENTION ANYTHING IN THE PRIVACY POLICY ABOUT THIS PARTICULAR DATA TYPES.
SO THAT'S ONE OF THE INTERESTING FINDINGS THAT WE DID.
FEW MORE OTHER INTERESTING AND ON THE PAPER, WE WILL NOT HAVE TIME TO COVER THEM.
BUT THEN WE DID MAKE SOME

OBSERVATION AND DID TRY TO MAKE
SOME RECOMMENDATIONS AND BASED
ON WHAT WE FOUND, AND ONE OF THE
INDICATIONS RECOMMENDATIONS IS
THAT A LOT OF THE USERS DID NOT
BE -- DID NOT UNDERSTAND THE
DIFFERENCE BETWEEN A NATIVE
SKILL AND THIRD PARTY SKILLS
JUST BY LOOKING AT IT IN THE
PUBLIC SKILLS STORE PAGE.
SO WE THINK SKILL TYPE IS
SOMETHING THAT WOULD BE USEFUL.
WE ALSO FEEL THAT VALIDATING THE
DEVELOPER RECOMMENDATION IS AN
IMPORTANT FACTOR HERE ESPECIALLY
AS IT ENABLES PHISHING ATTACKS
EVEN WHEN THE SKILLS ARE
SUBMITTED YOU HAVE TO SUBMIT THE
VARIOUS ATTEMPTS THIS IS WHERE I
THINK ALEXA OR AMAZON CAN COULD
A BETTER JOB IN VALIDATING THE
ATTEMPT TYPES, ANOTHER THING WE
SAW IN THE ENFORCEMENT OF A
PRIVACY POLICY IS NOT ALWAYS
USEFUL, SO WE BELIEVE THAT A
BETTER APPROACH WOULD BE TO HAVE
TO HAVE A PRIVACY POLICY
TEMPLATE BUILT INTO THE
SUBMISSION WHERE THE DEVELOPERS
WILLSHAVE TO EXPLICITLY SAVE THE
TYPE OF TODAY ACCESSING, PURPOSE
AND MAYBE USER USER HAD CHOICES.
THAT'S SOME OF THE
RECOMMENDATIONS WE MADE.
AND SO WE DID DISCLOSE OUR
FINDINGS AND HAD MULTIPLE
INTERACTIONS BUT WE DID SEE SOME
SKILLS REMOVED BUT WE DON'T KNOW
IF THAT IS THE RESULT OF OUR
RESEARCH OR ANY OTHER RESEARCH
HAPPENING WITH THE DEVELOPER
SIMPLY REMOVED THE SKILLS
THEMSELVES.
SO BUT WE HAVE MADE OUR DATA SET

PUBLIC.
AND THE WEBSITE ALSO HAS DEMOS OF SOME OF THE THINGS I JUST DISCUSSED TODAY.
IF YOU'RE INTERESTED I WOULD ENCOURAGE TO YOU VISIT THAT WEBSITE, LOOK AT SOME OTHER FINDINGS.
SO WITH THAT, I'LL END AND THANK MY CO AUTHORS LISTED HERE IF YOU HAVE FURTHER QUESTIONS ABOUT ANY OF THE FINDINGS THAT WE HAVE, WE'LL BE MORE THAN HAPPY TO ANSWER ANY OTHER QUESTIONS YOU MAY HAVE.
WITH THAT, I THINK I'LL END
>> I WASN'T, ANUPAM, THAT WAS GREAT.
NEXT WE'LL HEAR IN JEFFREY YOUNG PURSUING HIS PHD IF COMPUTER SCIENCE AT CLEMSON UNIVERSITY.
HE'LL PRESENT MEASURING THE POLICY COMPLIANCE OF VOICE ASSISTANT APPLICATIONS.
>> THANK YOU, TODAY, I'LL BE TALKING ABOUT OUR MEASURING THE POLICY COMPLIANCE VOICE ASSISTANT APPLICATIONS.
SO IF YOU CAN CLICK TO THE FIRST LINE.
SO THE FIRST THING I'D LIKE TO DO IS JUST KIND OF SET UP SOME DEFINITIONS.
SO WHAT IS A VOICE PERSONAL ASSISTANT?
OR VPA?
VPA ACTUALLY IS THE SOFTWARE THAT RUNS ON SMART SPEAKERS SUCH AS AMAZON'S ECHO AND GOOGLE'S HOME.
THE VPA ITSELF IS USUALLY NAMED SEPARATELY LIKE ALEXA, AND FOR THIS WORK, WE ANALYZE THE TWO MOST POPULAR VPA's WHICH IS FOR

GOOGLE HOME AND FOR THE AMAZON ALEXA TO SHOW THE POPULARITY OF THESE DEVICES, CURRENTLY THERE ARE OVER 128 MILLION SMART SPEAKER USERS IN THE UNITED STATES ALONE.
AND THE VPA ITSELF RUNS ON OTHER SOFTWARE SIMILAR TO CELL PHONE APS.
VPA THESE APPLICATIONS ARE CALL SKILLS FOR AMAZON AND CALLED ACTIONS FOR GOOGLE FOR REMAINDER ER OF THIS PRESENTATION I'LL REFER TO VOICE APS AND SKILLS FOR SIMPLICITY.
SKILLS LIKE CELL PHONE APS ARE CREATED BY THIRD PARTY DEVELOPERS.
SO BOTH AMAZON AND GOOGLE DO NOT PUT STIPULATIONS ON WHO CAN CREATE PUBLISHED SKILLS.
BUT THESE SKILLS DO GO THROUGH VETTING PROCESS ON BOTH PLATFORMS.
AND FOR SKILLS THAT PASS, THEY'RE PUBLISHED TO A SKILLS STORE, SO YOU KNOW, ON THE INTERNET, THERE'S A LOT OF DIFFERENT INFORMATION REGARDING DEVELOPED SKILLS.
FOR THE PURPOSE OF SECURITY, VPA PROVIDERS HAVE CREATED A SET OF POLICIES THAT SKILL DEVELOPERS SHOULD ADHERE TO.
AND JUST FOR A QUICK EXAMPLE, THERE ARE OVER 50 CONTENT POLICIES FOR AMAZON ALONE.
SO IN THIS WORK, BASICALLY WHAT WE DID WAS CONDUCTED A LARGE SCALE TESTING OF SKILLS ON THESE POLICIES TO SEE THEIR COMPLIANCE TO THESE DIFFERENT POLICIES THAT WERE SET UP BY THE VPA VENDORS, IF YOU COULD CLICK BASICALLY

HERE, YOU KNOW, IT'S RECENT RESEARCH IS SHOWING THE VPA VETTING PROCESS CAN BE WEAK AND SECURITY AND PRIVACY ISSUES EXIST, WE'RE INTERESTED IN THE POLICY COMPLIANCE DEPLOYED SKILLS CURRENTLY RUNNING ON THE AMAZON AND GOOGLE SKILLS STORES. SO THAT'S WHAT WE LOOKED AT IN THIS WORK.
NEXT LINE.
SO HERE ARE SOME EXAMPLES OF POLICIES PUT IN PLACE ON THE AMAZON PLATFORM, WE CONSIDER THEM HIGH RISK BECAUSE OF THE SUBJECT MATTER THEY DEAL WITH, KIDS AND HEALTH, IF YOU CAN SEE HERE, YOU KNOW, IN THE KIDS SECTION OF THE POLICY IS COLLECT ANY PERSONAL INFORMATION FROM END USER, WHICH WOULD BE CHILDREN.
OF COURSE, IT'S NOT ALLOWED -- THIS IS FOR THE AMAZON PLATFORM. PROMOTES PRODUCTS CONTENT SERVICE OR DIRECTS END USERS TO ENGAGE WITH CONTENT OUTSIDE OF ALEXA.
MOST DATA COLLECTIONS FOR KIDS IS PROHIBITED BY THE WAY OVER THIS PLATFORM.
CONTENT PRESENTED TO CHILDREN IS ALSO OF PARTICULAR INTEREST AS WELL AS PROMOTING CONTENT OUTSIDE OF THE PLATFORM.
SO ANYTHING THAT IS PROMOTED NOT WITHIN THE ALEXA ECOSYSTEM.
MOST HEALTH DATA IS PRICKEDED FROM COLLECTION.
ALSO GIVING HEALTH ADVICE OR INFORMATION MUST COME FROM A DISCLAIMER, MUST COME WITH A DISCLAIMER STATING THAT THIS MATERIAL IS NOT -- NOT SUITABLE

FOR ACTUAL MEDICAL ADVICE.
SO JUST TO GIVE AN OUTLINE OF HOW SKILLS WORK, THIS IS A BASIC SKILL INTERACTION, THIS IS A HIGH LEVEL VIEW OF HOW THE SKILL WORKS.
SKILL INTERACTION STARTS WITH AN UTTERANCE, AND THAT'S, FOR EXAMPLE, WOULD BE ALEXA OPEN ABC.
SOME SKILL, FOR SOME SKILLS

PERMISSION GRANTED VIA AN ON A CELL PHONE.
THEY CAN BE MANY SKILLS OF A CERTAIN TYPE.
NEXT DEVICE CAPTURES THE AUDIO FILES OF THE USER, WHATEVER IS VERBALLY SPOKEN INTO THE DEVICE, SENDS TO THE CLOUD TO BE PROCESSED.
IT IS HERE THAT A SKILLS FRONT END CODE IS HOUSED ON THE CLOUD.
FROM THE CLOUD, THE INTERACTION DATA CAN BE SENT TO THE SKILLS BACK END CODE, WHICH CAN BE HOSTED OUTSIDE OF THE VPA PLATFORM.
THIS IS WHAT MAKES TRADITIONAL STATIC CODE ANALYSIS FOR SKILLS NOT POSSIBLE AND BASICALLY SERVES AS A BLACK BOX, WE REALLY DON'T KNOW WHAT'S GOING OF THE SKILLS.
ALSO, IT IS THE BACK END THAT PROVIDES MOST OF THE CONTENT OF THE SKILL WHICH CAN INCLUDE AUDIO FILES, IMAGES AND TEXTS.
SO BECAUSE A LARGE PORTION OF THE SKILLS SOURCE CODE IS HOSTED EXTERNALLY ALL WE HAVE TO ANALYZE IS THE SKILL'S FUNCTIONALITY, HOW THE SKILL INTERACTS, WHAT THE SKILL ACTUALLY WHAT WE LOOK AT.

NEXT LINE.
HERE ARE THE CONTRIBUTIONS SOME
OF THE CONTRIBUTIONS OF THIS
WORK.
SO WE DESIGNED AND DEVELOPED THE
DYNAMIC TESTING TOOL NAMED SKILL
DETECTIVE.
IT'S BASICALLY LIKE A CHAT BOX
MODEL THAT INTERACTS WITH THE
ECHO DEVICE AND THE GOOGLE
DEVICE.
WE CONDUCTED A COMPREHENSIVE
DYNAMIC AND STATISTIC ANALYSIS
OF SKILLS TO DETECT IF THEY
FOLLOW CURRENT POLICIES OF THE
VPA PLATFORMS, SO FROM THE
INTERACTION DATA THAT WE
COLLECT, WE COULD DETERMINE
POLICY VIOLATION AND AFTER OVER
A YEAR OF DEVELOPMENT AND
TESTING WE HAVE TESTED 54,055
AMAZON ALEXA SKILLS AND 5583
GOOGLE ASSISTED ACTION, I WOULD
LIKE TO MANY THERE'S MANY MORE
AMAZON ALEXA SKILLS PUBLISHED
THAN THAT OF THE GOOGLE ACTION,
ALSO GOOGLE MAKES IT MORE
DIFFICULT TO INTERACT WITH ITS
PLATFORM USING WEB DRIVERS.
SO FOR SOME REASON, SO THE MAKES
IT MORE DIFFICULT TO ACTUALLY
TEST GOOGLE ACTIONS.
SO THIS IS THE SKILL DETECTIVE
OVERVIEW.
I WILL BRIEFLY GO OVER THIS BOTH
AMAZON AND GOOGLE CREATED, TAKES
THE TEXTING INPUT TRANSCRIBES
THE VOICE OF THE DEVICE INTO
TEXT, YOU WILL RECEIVE A TEXT
RELAY OUTPUT , UNFORTUNATELY IT
WILL NOT TRANSCRIBE AUDIO FILES,
IF THE OUTPUT IS STRICTLY AUDIO
FILES, GIVES YOU A MESSAGE SAYS
IT'S JUST AN AUDIO FILE.

SO WE HAVE TO TRANSCRIBE THOSE SEPARATELY.
FIRST, WE CREATED THE SAMPLE UTTERANCES FROM DIFFERENT SKILL STORES, THESE ARE USED TO BEGIN THE SKILL INTERACTION BY INVOKING THE DEVICE, SO WE MONITORED THE SKILL STORES AND COLLECT ADD DATA SET OF ALL THE SAMPLE UTTERANCES, SECOND, THE SKILL DETECTIVE COLLECTS THE INITIAL SKILL OUTPUT AND SENDS IT TO THE INTERACTION MODEL.
HERE SKILL DETECTIVE TERMS IF THE OUTPUT CONTAINS A QUESTION, IF SO, WE'LL PREDICT THE ANSWER TO THE QUESTION.
SO THIS IS DONE BECAUSE THESE ARE VERBAL MACHINES, SO YOU HAVE TO BE ABLE TO TALK BACK AND FORTH IN ORDER TO GATHER AS MUCH OUTPUT AS YOU POSSIBLY CAN FROM EACH INDIVIDUAL SKILL.
SO NEXT THE ANSWER WOULD BE SENT BACK TO TRIGGER THE NEXT OUTPUT AND THIS PROCESS GOES ON UNTIL WE HAVE EXHAUSTED THE SKILL.
WE CALL THIS BACK AND FORTH SKILL NAVIGATION.
SO WE'RE NAVIGATING THE SKILL.
BASICALLY SKILL DETECTIVE CARRIES ON A CONVERSATION WITH THE SMART SPEAKER AND RECORDS ALL THE INTERACTION.
SO DURING SKILL NAVIGATION, SKILL DETECTIVE CREATES A MAP OF THE ACCIDENT BY KEEPING TRACK OF THE OUTPUTS AND THE OUTPUT TYPES.
SO THAT THE SKILL CAN BE THOROUGHLY EXPLORED.
AND DURING ALL THE SKILL INTERACTION, THE SYSTEM COLLECTS ALL THE DATA TYPES OF OUTPUT BY

THE SKILLS.
THIS INCLUDES IMAGES, AUDIO FILES AND TEXTS.
AND LASTLY, THE INTERACTION DATA ITSELF IS ANALYZED FOR POLICY COMPLIANCE.
SO WE LOOK AT ALL THE DATA WE'VE COLLECTED FROM EACH SKILL SEPARATELY.
NEXT SLIDE.
SO AUTOMATING THE POLICY VIOLATION DETECTION, SO WE CHECKED BASICALLY FIRST THIS -- THIS IS A PAGE TAKEN FROM THE SKILLS STORE FOR A SPECIFIC SKILL, WEALTHY NUTRITION.
WE CHECKED THE CATEGORY TO DETERMINE WHICH POLICIES APPLIED TO EACH GIVEN SKILL, SO FIRST WE WANT TO KNOW IF IS THE SKILL LIKE IN THE KIDS CATEGORY LIKE CERTAIN POLICIES WOULD APPLY -- WOULD NOT APPLY TO OTHER SKILLS?
NEXT WE CHECK IF THE SKILL HAS ANY MISSING PERMISSIONS, SO SHOULD THE SKILL HAVE A PERMISSION SET LIKE COLLECTS DATA OR SOMETHING LIKE THAT, AND WE CAN ANALYZE THE SKILLS OUTPUT AND DETERMINE IF IT DOES COLLECT THIS DATA AND IF SO, ARE THE PERMISSIONS HANDY ON THE WEBSITE.
WE ALSO CHECKED FOR INCONSISTENT.
WE TRANSCRIBE TO CHECK FOR POLICY VIOLATIONS AND ANALYZE IMAGES FOR POTENTIAL POLICY VIOLATION, SO OVERALL, WE CHECK FOR OVER 40 DIFFERENT POLICY VIOLATIONS ON THE DIFFERENT PLATFORMS.
SO HERE'S SOME EVALUATION RESULTS.

SO WE IDENTIFIED 6,079 SKILLS
AND 175 ACTIONS POTENTIALLY
VIOLATING THE AT LEAST ONE
POLICY REQUIREMENT.
590 SKILLS IN 24 ACTIONS OF
THOSE ACTIONS VIOLATE MORE THAN
ONE POLICY.
IN THE KIDS CATEGORY, WE
IDENTIFIED 244 POLICY VIOLATING
SKILLS.
AND 80% OF THE SKILLS AND 68% OF
ACTIONS IN THE HEALTH CATEGORY
POTENTIALLY VIOLATE AT LEAST ONE
POLICY.
623 SKILLS AND 25 ACTIONS
POTENTIALLY VIOLATE POLICIES
RELATED TO PERSONAL DATA CHECK.
SO THESE ARE SOME OF THE RESULTS
WE FOUND SO FAR IN OUR TESTING.
SO HERE WE HAVE SOME EXAMPLES OF
POLICY VIOLATIONS, WHAT WE
FOUND, AS YOU CAN SEE, THIS IS,
YOU WILL SEE THIS IS THE, THE
ALEXA TESTING CONSOLE WE'RE
INTERACTING WITH.
SO THE FIRST ONE HERE IS
COLLECTING PERSONAL DATA AND AS
YOU CAN SEE, IT SAYS PLEASE TELL
ME YOUR NAME.
THIS SKILL, NORMALLY WOULD NOT
BE IN VIOLATION BUT IT'S IN THE
KIDS' CATEGORY.
SO BECAUSE IT'S IN THE KIDS'
CATEGORY, IT ASKS TO COLLECT --
IT ASKS FOR THE CHILD'S NAME OR
THE USERS NAME.
NEXT ON THE EXAMPLES.
ALSO HERE'S SOME -- AN EXAMPLE
OF EXPLICIT OR MATURE CONTENT
AND TOXIC CONTENT, SO I WON'T
READ WHAT IT IS, BUT IF YOU
COULD READ IT FOR YOURSELF.
THEN THERE'S THE NEXT EXAMPLE
HERE IS REQUESTING A POSITIVE

RATING.
WHICH IS ACTUALLY A VIOLATION,
AND THAT IS -- THAT IS DONE,
TOO, BECAUSE THE RATINGS ARE
USED -- ARE IT'S THOUGHT THAT
THE RATINGS ARE USED TO
DETERMINE WHICH SKILL IS
SELECTED FOR AND DURING
INVOCATION.
NEXT SLIDE.
SO HERE'S THE FEW KEYS TO
EVALUATION, SO WE ANALYZE THE
KIDS CATEGORY ON THE ALEXA
PLATFORM.
AND THESE ARE RESULTS.
COLLECTING DATA AND KIDS, WE
FOUND THAT 34 OUT OF 3,617
SKILLS COLLECT DATA.
21 SKILLS DIRECTED USERS TO
OUTSIDE OF THE ALEXA PLATFORM.
12 SKILLS HAD EXPLICIT OR MATURE
CONTENT FOR CHILDREN.
177 SKILLS REQUESTED A POSITIVE
RATING.
WE FOUND FOUR SKILLS THAT HAD
TOXIC CONTENT, AND WE FOUND 244
SKILLS TOTALING -- 244 TOTAL
POLICY VIOLATING SKILLS FOR THE
ALEXA KIDS SECTION.
NOW, IF YOU SEE IN CONTRAST, THE
GOOGLE ACTION SECTION, WEuL)Ñ --
SOME OF THE REQUESTING POSITIVE
RATING DOES NOT APPLY, AND
DIRECTING USERS OUTSIDE OF
GOOGLE DOES NOT APPLY.
AND WE ACTUALLY FOUND NO
VIOLATIONS IN THE KIDS CATEGORY.
BUT AGAIN, IF YOU LOOK AT THE
DIFFERENCE, THE YOU KNOW,
BETWEEN 3,617 SKILLS AND 108
ACTIONS ALL THAT THERE WAS AT
THE TIME WE COLLECTED THE DATA.
SO HERE'S THE NONKIDS EVALUATION
RESULTS.

SO WE FOUND TOTALLY 3,464 SKILLS COLLECTED ARE REQUESTED A POSITIVE RATING.
1,709 SKILLS IN THE HEALTH CATEGORY, WE'RE LACKING A DISCLAIMER AT 79% OF THE HEALTH CATEGORY, IN CONTRAST, 151 OR 66% OF ACTIONS LACK THE DISCLAIMER IN THE HEALTH CATEGORY, 146 SKILLS COLLECT HEALTH DATA WHEREAS 13 ACTIONS COLLECT HEALTH DATA.
THREE WERE DIRECTING USERS OUTSIDE OF ALEXA THIS WAS ACTUALLY FOUND IN IMAGE OR AUDIO FILES.
TWO WERE LACKING PRIVACY POLICY, THIS ALSO IN THE IMAGE OR AUDIO.
AND INCOMPLETE PRIVACY POLICY TWO SKILLS, NO ACTIONS.
SO IF YOU COULD CLICK TO THE NEXT SLIDE.
THIS BASICALLY THE END WE REPORTED THE RESULTS TO AMAZON AND GOOGLE AND GOT THEIR ACKNOWLEDGEMENT.
WE HAVE FOUND GOOGLE CONFIRMED THAT 43 OUT OF 175 ACTIONS WERE IMMEDIATELY REMOVED FROM THE STORE BECAUSE OF OUR REPORTING.
AND THE REMAINING ACTIONS WERE DEEMED TO HAVE NOT BEEN IN VIOLATION OR THE POLICY VIOLATION ONLY WARRANT ADD WARNING RATHER THAN A TAKE DOWN
SO WE REPORTED EVERYTHING TO AMAZON AND THEY HAVE -- WE HAVE NOT VALIDATED ANYTHING LIKE THIS WITH THEM.
SO THAT'S IT.
THANK YOU VERY MUCH.
THAT WOULD BE THE END OF IT
>> THANK YOU, JEFFREY, NOW WE WILL HEAR FROM PARDIS

EMAMI-NAENI.
FROM THE UNIVERSITY OF WASHINGS
AS PART OF HER DOCTORAL RESEARCH
SHE DEVELOPED A PRIVACY AND
SECURITY LABEL FOR SMART DEVICES
CONTINUED THIS IN HER CURRENT
PAPER AND WILL PRESENT ON WHICH
PRIVACY AND SECURITY ATTRIBUTES
MOST IMPACT CONSUMER'S RISK AND
PERCEPTION AND WILLINGNESS TO
PURCHASE IOT DEVICES.
>> THANK YOU VERY MUCH.
LINDA, HI, EVERYONE, THANK YOU
FOR JOINING MY TALK, I'M PADRES
EMAMI-NAENI AT UNIVERSITY OF
WASHINGTON.
TODAY I'M GOING TO TALK ABOUT
OUR PROJECT IDENTIFY HOW PRIVACY
AND SECURITY FACTORS IMPACT IOT
CONSUMERS RISK PERCEPTION AND
WILLING TO PURCHASE, THIS HAS
BEEN CONDUCT WHILE DOING MY PHAT
CARNEGIE.
MANY OF US HAVE THE EXPERIENCE
OF PURCHASING THIS SMART DEVICE
FOR OURSELVES OR OTHERS.
NOW, I WANT TO TO REMEMBER A
TIME WHEN YOU WERE IN A PHYSICAL
STORE OR SEARCHED ONLINE FOR A
SMART DEVICE, YOU PROBABLY SAW
INFORMATION ON THE PRICE OF THE
DEVICE OR TECHNICAL
SPECIFICATIONS, FOR EXAMPLE,
SIZE OR INTERNET CONNECTIVITY DO
YOU REMEMBER SEE ANY INFORMATION
ABOUT PRIVACY AT THE TIME OF
PURCHASE?
PROBABLY NO.
BECAUSE USUALLY THIS INFORMATION
IS NOWHERE TO BE FOUND.
PURCHASING A SMART DEVICE ON
LINE OR IN A STORE CONSUMERS ARE
NOT ABLE TO MAKE AN INFORMED
PURCHASE DECISION AS INFORMATION

ON THE SECURITY AND PRIVACY
BEHAVIOR OF THE SMART DEVICES,
IS NOT AVAILABLE TO THEM.
TO HELP AN INFORMED CONSUMER'S
PURCHASED DECISION MAKING
PROCESS, WE DESIGNED AN IOT
PRIVACY AND SECURITY LABEL,
SOMEWHAT SIMILAR TO THE
NUTRITION LABELS FOR FOOD ITEMS,
WE TALKED ABOUT THE DETAILS OF
THE LABEL IN OUR OPEN 2020, OUR
LABEL HAS TWO LAYERS, A PRIVATE
AND SECOND LAYER THAT CAN BE
ACCESSED THROUGH THE PRIOR LAYER
BY STANDING THE CODE OR TYPING.
WE DESIGNED THEY DIDN'T LABEL
MAINLY BASED ON INPUTS FROM
EXPERTS FROM ACADEMIA INDUSTRY,
GOVERNMENT.
FROM THE LITERATURE, WE KNOW
THAT EXPERTS UNDERSTAND IT COULD
BE DIFFERENT FROM CONSUMERS IT'S
IMPORTANT THAT THE LABEL CONVEYS
TO ACCURATELY FOR THEIR
WILLINGNESS TO PURCHASE THE
SMART DEVICE.
TO ASSESS THIS WE CONDUCTED AN
ONLINE STUDY FOR THE PURPOSE OF
THIS TALK.
NEXT.
IN OUR SURVEY, WE ASKED
PARTICIPANTS TO IMAGINE
PURCHASING A SMART DEVICE FOR
THE PRIVACY AND SECURITY LABEL.
LABEL TALKED ABOUT ONLY ONE
PRIVACY OV SECURITY ATTRIBUTE.
EACH WAS ASSIGNED TO ANSWER
QUESTIONS RELATED TO THREE
PURCHASE SCENARIOS.
THIS IS AN EXAMPLE OF A SCENARIO
THAT PRESENTED TO PURCHASE.
THE INSIDE THE BRACKETS ARE THE
FACTORS IN THE SCENARIOS.
IMAGINE YOU'RE MAKING A DECISION

TO PURCHASE A SMART SPEAKER ASSIST FOR YOURSELF, THIS HAS A MICROPHONE THAT WILL LISTEN AND RESPOND TO VOICE COMMANDS, THE PRICE AND THE FEATURES ARE ALL WHAT YOU WOULD EXPECT FROM A SMART SPEAKER SYSTEM.
ON THE PACKAGE OF THE DEVICE, THERE'S A LABEL THAT INDICATES THE PRIVACY AND SECURITY PRACTICE.
PURPOSE UPDATE COLLECTION, PAY ADVERTISING.
AT THE END OF EACH SCENARIO WE ASKED PARTICIPANTS TO SPECIFY ON LARGER SCALE HOW EACH ATTRIBUTE'S VALUE WOULD CHANGE THE RISK PERCEPTION AND WILLINGNESS TO PURCHASE AND WHY.
AT THE BEGINNING OF MY TALK I SHOWED YOU THE LAYER LABEL THAT PREVIOUSLY DESIGNED FROM INFRASTRUCTURE EXPERTS.
IN THIS STUDY, THEY SELECTED A SUBSTANCE OF THE LABEL FACTORS TO ASSESS.
FOR EACH ATTRIBUTE, WE SELECTED TWO VALUES, HYPOTHESIZE TO BE THE MOST PROTECTIVE AND THE LEAST PROTECTIVE.
FOR EXAMPLE, FOR PURPOSE OF DATA COLLECTION, THOSE PROVIDING MAIN DEVICE FUNCTION AS THE MOST PROTECTIVE VALUE AND MONTE SENSATION AS THE LEAST.
THE HYPOTHESIZE THAT THE MOST PROTECTED VALUE OF ATTRIBUTES SHOULD SIGNIFICANTLY DECREASE THE RISK AND INCREASE THE PURCHASE.
WE EXPECTED THE OPPOSITE FOR THE LEAST PROTECTED VALUES.
AMAZON MECHANICAL: THIS STATISTICAL MODELS INDICATED THE

IMPACT OF ALMOST ALL SCORNED ATTRIBUTE VALUES ARE RISK PERCEPTION WILLINGNESS TO PURCHASE, MEANING HYPOTHESIZE MOST PROTECTED VALUES SIGNIFICANTLY DECREASE THE PERCEIVED RISK AND INCREASE WILLINGNESS TO PURCHASE AND THE LEAST PROTECTIVE VALUE, SIGNIFICANTLY INCREASED THE RISK PERCEPTIONS AND DECREASED THE DESIRE TO PURCHASE THE SMART DEVICE.
THERE WERE A FEW EXCEPTIONS.
THE FACTOR PROFICIENT.
WE FOUND THE EFFECTIVENESS OF ATTRIBUTES IN TERMS OF CHANGING PARTICIPANTS RISK PERCEPTION AND WILLINGNESS TO PURCHASE.
STARTED WITH THE RISK PERCEPTION, THE TOP THREE ATTRIBUTES THAT SIGNIFICANTLY INCREASE THE PERCEIVED RISK, SHARING DATA WITH THIRD PARTIES PROVIDING NO CONTROL OVER ACCESS AND SELLING DATA TO THIRD PARTIES.
ON THE OTHER END OF THE SPECTRUM, THE TOP THREE ATTRIBUTES THAT DECREASED THE RISK PERCEPTION WERE MULTI-FACTOR THANKS SHARING DATA WITH NOBODY AND HAVING NO CLOUD RETENTION.
IN TERMS OF WILLINGNESS TO PURCHASE, WE FOUND VERY SIMILAR TRENDS.
THE TOP THREE FACTORS TO INCREASE PARTICIPANTS DESIRE TO PURCHASE THE SMART DEVICE, NO DEVICE RETENTION, NO CLOUD RETENTION AND SHARING DATA WITH NO ONE.
AND THE TOP THREE TO DO I CREASE

THE WILLINGNESS OF PURCHASE, SHARING DATA WITH THIRD PARTIES HAVING NO ACCESS CONTROL AND SELLING DATA TO THIRD PARTIES.
THE OPEN EXPLANATIONS HELP US IDENTIFY SEVERAL REASONS AS TO WHY SOME PARTICIPANTS RISK PERCEPTION AND WILLINGNESS TO PURCHASE WERE DIFFERENT FROM WHAT YOU HAVE HYPOTHESIZED.
STARTING WITH THE AVERAGE TIME TO PATCH THESE ARE GUIDELINES IN OUR STUDY WE SELECTED THE MOST PROTECTIVE VALUE OF THIS ATTRIBUTE TO BE ONE MONTH.
AND LEAST PROTECTED VALUE TO BE SIX MONTHS.
IN OUR MODELS, BOTH VALUES SIGNIFICANTLY INCREASE THE PURCHASE AND DECREASE THE WILLINGNESS TO PURCHASE.
IT'S THE, IT INDICATES THE IMPACT OF THE ATTRIBUTE VALUES AND THE YAXIS SHOWS THE IMPACT ON WILLSNESS TO PURCHASE.
BLUE POINT PRESENTS THE MOST PROTECTED VALUE IN THIS CASE ONE MONTH AND THE RED DOTS PRESENT THE LEAST PROTECTED VALUE, HERE SIX MONTHS.
AS YOU CAN SEE, MOST OF THE BLUE AND RED DOTS ARE CLUSTERED IN THE RIGHT.
SHOWING AN INCREASED IN RISK PERCEPTION AND DECREASE IN WILLINGNESS TO PURCHASE.
S A BEST PRACTICE, MANUFACTURERS SHOULD PATCH IN THE SHORTEST TIME.
SOMETIMES, DEPENDING ON VARIOUS FACTORS, IT COULD TAKE LONGER TO, A PATCH OR FINALLY SUGGEST THAT MANUFACTURERS NEED TO PROVIDE CONSUMERS WITH

JUSTIFICATIONS AS TO WHY IT TAKES THEM A SPECIFIC AMOUNT OF TIME AND WHY PATCH THE ABILITIES FASTER.
PURPOSE OF DATA COLLECTION WAS ANOTHER FACTOR THAT DID NOT CHANGE THE PURCHASE PERCEPTION AND WILLINGNESS TO PURCHASE AS WE EXPECTED.
ALTHOUGH THE HYPOTHESIZED THAT PROVIDING DATA FOR DEVICE FUNCTIONALITY SHOULD DECREASE THE PERCEIVED RISK, THAT WAS TRUE FOR ONLY 12% OF PARTICIPANTS.
OTHER PARTICIPANTS STATED THAT THIS INFORMATION WOULD NOT IMPACT RISK PERCEPTION OR WOULDN'T INCREASE THE RISK MOSTLY DUE TO LACK OF TRUST IN MANUFACTURERS, A PARTICIPANT MENTIONED THAT COMPANIES HOOK LIKE DATA ARE INCREDIBLY UNTRUSTWORTHY, DO NOT HAVE CONSUMERS BEST INTEREST IN MIND, UTILIZING THE DATA THEY COLLECT.
WE ALSO NOTICED A FEW PRIVACY MISCONCEPTIONS.
FOR EXAMPLE, SOME PARTICIPANTS THOUGHT THAT NO SECURITY UPDATES INDICATE BETTER SECURITY AS THE DEVICE DOES NOT NEED TO BE UPDATED.
PARTICIPANTS SAID IF THERE ARE NO UPDATES THEN THE SYSTEM MUST BE PROVIDING MAXIMUM SECURITY ALREADY.
ANOTHER MISCONCEPTION WAS RELATED TO MENTIONING THE AVERAGE TIME TO PATCH.
SOME PARTICIPANTS BELIEVE THAT EVEN MENTIONING THE WORD PATCH INDICATES THAT THE DEVICE IS NOT SECURE.

AS IT NEEDS TO BE PATCHED A
PARTICIPANT SAID AND THE LABEL
IT ADVERTISES THAT PATCHES ARE
EVEN NEEDED.
THAT IS WHY THERE IS A
PERCEPTION OF DECREASED PRIVACY.
TO RECAP, WE EXPLORED THE
EFFICACY OF OUR PREVIOUSLY
DESIGNED IOT PRIVACY LABEL IN
CONVEYING RISK TO CONSUMERS AT
INFLUENCING THEIR WILLINGNESS TO
PURCHASE.
TO DO SO, WE ASSESSED THE IMPACT
OF A SUBSET OF LABEL PRIVACY AND
SECURITY FACTORS AND CONDUCTED A
LARGE SCALE LIVE STUDY WE FOUND
IN MOST CASES, THE LABEL WAS
EFFECTIVE TO CHANGE CONSUMER'S
RISK PERCEPTION AND INFORMED
WILLINGNESS TO PURCHASE.
HOWEVER, WE FOUND A FEW
EXCEPTIONS.
CODING THE OPEN END OF THE
PROCESS THE SURFACE PURCHASE THE
MISCONCEPTIONS THAT IMPACTED THE
RISK PERCEPTION AND WILLINGNESS
TO PURCHASE.
IF YOU WANT MORE INFORMATION
ABOUT OUR LABEL PROJECT AND SEE
HOW YOU CAN HELP WITH THE
EFFORT, PLEASE VISIT
IOTSECURITI.ORG.
I'M PARDIS EMAMI-NAENI AND THANK
YOU FOR YOUR ATTENTION.
>> THANK YOU, PARDIS, LAST BUT
DEFINITELY IN THE LEAST WE WILL
HEAR FROM GENEVIEVE LIBERTE,
FROM THE FLORIDA WHERE SHE WORKS
AT THE SECURITY LAB, SHE WILL
ON HER PAPER, REALLY-TIME
ANALYSIS OF PRIVACY UNAWARE IOT
APPLICATIONS.
>> GOOD AFTERNOON, MY NAME IS
GENEVIEVE LIBERTE THE TITLE OF

THIS IS REALLY TIME ANALYSIS OF PRIVACY UNAWARE OF IOT APPLICATIONS IT WAS A JOINT EFFORT.
IT WAS RECENTLY PRESENT TO DO THE PRIVACY SYMPOSIUM OF 2021.
SO IN THE WORLD OF OF THE INTERNET OF THINGS OR IOT, USERS INSTALL IOT APPLICATIONS TO MANAGE AND CONTROL SMART DEVICES LIKE THERMOSTATS, SMART LOCKS AND CAMERAS.
APS NECESSARILY HAVE ACCESS TO SOME DATA TO IMPLEMENT FUNCTIONALITY, COMMUNICATE WITH EXTERNAL SERVERS AND SEND NOTIFICATIONS TO USERS, HOWEVER THIS ACCESS IS TO SENSITIVE DATA CAN HAVE NEGATIVE PRIVACY IMPLICATIONS SOME IOT APS HAVE BEEN SHOWN TO LIKE SENSITIVE INFORMATION TO UNAUTHORIZED PARTIES AND MANY TRANSMIT TO PROMOTE VISUALIZATION AND PROFIING DESPITE ENTRUSTING APS USERS HAVE LITTLE KNOWLEDGE OR CONTROL WHAT SENSITIVE DATA LEAVES THE APS OR SHOWN TO THIRD PARTIES.
ON THE LEFT OF THIS SLIDE WE SEE AN PORTION OF AN EXAMPLE OF A SOURCE CODE WRITTEN IN PROGRAMMING LANGUAGE, AP SOURCE CODE TYPICALLY INCLUDES A DESCRIPTION BLOCK YOU CAN SEE AT COAT THE POINT ONE THIS AP DESCRIPTION BLOCK IS VAGUE DOESN'T DO A GREAT JOB TO DESCRIBE HOW THE INFORMATION WILL BE UTILIZED OR SHARES, DURING INSTALLATION, THE USER WILL GRANT PERMISSIONS TO THE AP AND AUTHORIZE SPECIFIC RECIPIENTS FOR NOTIFICATION

PURPOSES WHICH WILL POPULATE THE PERMISSIONS BLOCK VARIABLES.
TO SUPPORT THING FUNCTIONALITY, IT MAY INCLUDE FUNCTIONS WHICH TRANSMIT DATA OVER THE INTERNET, DESPITE NOT RECEIVING AUTHORIZATION FROM THE USER TO DO SO, THIS SORT OF BEHAVIOR CAN BE SEEN AT CODE POINT THREE,
IT'S POSSIBLE FOR AN APPLICATION TO HARD CODE ADDITIONAL RECIPIENTS TO SENSITIVE DATA. WITHOUT THE USER EVEN KNOWING. THIS CAN BE SEEN IN THE BEHAVIOR OF THE LEAKED INFO FUNCTION HERE AT CODE POINT FOUR.
FROM THE EXAMPLE ON THE PREVIOUS SLIDE, WE CAN EXTRAPOLATE FOR MAIN PRIVACY CHALLENGES THAT CONSTITUTE THE THREAT MODEL,
FIRST PRIVACY BEHAVIOR FROM APS, APS MAY ACCESS PROTEST INFORMATION WITHOUT THE OF USER'S CONSENT, NEXT SENSITIVE DATA MAY BE LIKED TO UNAUTHORIZED RECIPIENTS THROUGH MALICIOUS OR CARELESSLY DEVELOPED IOT APS, UNDISCLOSED OR MALICIOUS AP CONTENTS, APS MAY NOT PROPERLY INFORM USERS HOW DATA WILL BE USED OR REQUIRED.
FINALLY UNPROTECTED DATA FLOWS, APS MAY NOT LEAVING SENSITIVE DATA VULNERABLE WHEN TRANSFERRED OVER WIRE, WHEN LOOKING AT WAYS TO PROTECT AGAINST THESE, NONE OF THE MAJOR IOT PLATFORMS PROVIDED A WAY TO ANALYZE PRIVACY RISK OR INFORM USERS HOW SENSITIVE INFORMATION WILL BE UTILIZED.
THIRD, STATIC ANALYSIS WHICH MAY NOT CATCH INFORMATION LIKE

THROUGH HARD COATED RECIPIENTS.
OR USER DEFINED.
IN THINKING ABOUT A SOLUTION TO THE ISSUES WE WANTED TO ASK IF IOT USERS HOW THEY COULD BE BETTER SERVED BY POTENTIAL IOT PRIVACY TOOLS WE DESIGN ADD SURVEY ASKING THREE MAIN SUBJECTS THE EXPERIENCE AND DEMOGRAPHICS OF THE PARTICIPANT, THE PRIVACY CONCERNS THEY HAVE WITH IOT AND THE NEED FOR IOT PRIVACY ANALYSIS TOOLS IN THEIR USE ABILITY TO REQUIREMENTS WE HAD 112 PARTICIPANTS, MANY OF WHEN I AM BELONGED TO AN EDUCATIONAL INSTITUTION.
WE FOUND THAT OVER 2/3RDS PARTICIPANTS WERE CONCERNED ABOUT PERSONAL DATA, HABITS LOCATIONS AND DEVICE BEING HANDLED AND SHARED BY IOTAPS, MAJORITY OF USERS EXPRESSED CONCERNS ABOUT USING IOT SYSTEMS AND MANY AWARE PRIVACY ISSUES HOW TO NEWS STORIES OR OTHER MEDIA.
WHEN ASKED ABOUT THE IDEA THAT TOOLS MEMBER PRIVACY IN THE IOT SYSTEMS ALMOST 97% OF PARTICIPANTS FOUND THIS IDEA TO BE HIGHLY DESIRED AND EXPECTED.
REGARDING THEIR EXPECTATIONS FOR THIS IDEA, PARTICIPANTS EXPRESSED A SHARED DESIRE FOR A USER FRIENDLY TOOL COULD BE CONFIGURED WITH VARIOUS PRIVACY PREFERENCES AND PROVIDE REAL TIME NOTIFICATIONS WHEN PRIVACY THREATS ARE DETECTED.
TAKING INTO ACCOUNT THE FEEDBACK WE GOT FROM OUR SURVEY, WE ARRIVED AT OUR PROPOSED SOLUTION IOT WATCH.

IOT WATCH IS A DYNAMIC ANALYSIS
TOOL TO UNCOVER PRIVACY RISKS
THAT IOT RISKS POSE TO THE USERS
IN REAL TEAM.
IOT WATCH WORKS THREE STAGES,
INSTRUMENTATION TIME WHICH
HAPPENS BEFORE THE USER CAN
FIGURE THE PREFERENCES, INSTALL
TIME HAD WHICH THE USERS DEVICE
WHICH PRIVACY THEY WANT TO SEE
NOTIFICATIONS FOR AND RUN TIME
WHEN THE AP IS RUN ON THE SMART
DEVICE.
DURING THE INSTRUMENTATION
PROCESS THE ORIGINAL SOURCE CODE
IS IF HE DID TO THE IOT WATCH.
IT ANALYZES THE SOURCE CODE TO
DETERMINE HOW AND WHEN THIS
FUNCTION IS CALLED AND WHAT
VARIABLES MAY BE PASSED TO THEM.
IOT WATCH USES THIS TO INSERT
ITS OWN CODE NOT AP SO THE DATA
SENT OUT OF THE AP DURING RUN
TIME WILL BE SENT TO IOT WATCH
FOR ANALYSIS AND MATCHING WITH
THE USER PREFERENCES.
ONCE THE CODE IS INSTRUMENTED,
THE USER CAN FIGURE THEIR
PRIVACY PREFERENCES WITH
IOTWATCH GRAPHICAL USER
INTERFACES.
AFTER THIS, USER CAN BEGIN TO
USE THE AP NORMALLY DURING RUN
TIME, IOTWATCH COLLECTS THE
FUNCTION CALLED THE RESULT OF
DATA LEAVING THE TO DETERMINE
WHETHER ANY OF THESE SENSITIVE
DATA CAN BE LEAKED ACCORDING TO
THE USER'S ONLY CONFIGURATION,
IF DATA LIKES ARE FOUND,
IOTWATCH IS IMMEDIATELY SENT.
SO HOW DOES IOTWATCH SOURCE CODE
INSTRUMENTATION WORKS?
IT'S GENERATES VERSION OF THE

ORIGINAL SORE CODE.
MOST IOTAPS FOLLOW SIMILAR STRUCTURES EVEN ON DIFFERENT PROGRAMS AND USING THE INTERMEDIATE YET ALLOWS IT TO BE ON THE IOT PLATFORMS, FROM THIS INTERMEDIATE YET, WE'RE ABLE TO DETERMINE CODES.
WE IDENTIFY ALL OF THE PLACES AND CODE AT WHICH DATA EXITS THE AP TO BE TRANSMITTED, IOTWATCH SPECIFICALLY FOCUSES ON MESSAGING AND REINSTATE, WHERE IT'S SENSE OUT VIA INTERNET OR SMS, ALLOWING IT TO, WHICH ANALYZES VISITOR ALGORITHM.
IOT WATCH CAN IDENTIFY USER DEFINED INPUT IN THE APS PERMISSION BLOCK AS WELL AS RECIPIENTS AND CONTENTS.
IF CONTROL FLOW GRAPH IS ALSO WHAT ENABLES IOTWATCH TO ADD ITS OWN CODE.
THE EXTRA CODE COLLECTS AND TRANSMITS TO SERVER TO INFORM USERS ABOUT IOTWATCH ANALYSIS RESULT AND THE NEXT SLIDE, WE CAN TAKE A LOOK HOW IOTWATCH DATA COLLECTION WORKS IN MORE DETAIL.
SO ON THE RIGHT HERE WE HAVE OUR EXAMPLE, IOT AP AFTER BEING INSTRUMENTED BY IOT WATCH, AT .CONE, WE FIND USER PHONE NUMBER IN THE APS PERMISSION BLOCK, IT USES UPPERS TO DETERMINE IT'S LEGITIMATE WHICH HAS BEEN PROVIDED BY THE USER, AT POINTS IN THE CODE SINK HOLES OCCUR LIKE LINE C2 AND 4, IT ADDS ADDITIONAL CODE TO ANALYZE CALLS AND INFORM THE USER IF THESE LEAD TO VIOLATIONS OF THEIR PRIVACY PREFERENCES, FOR

INSTANCE THE LEFT IS AN EXAMPLE OF THE USER CONFIGURED PRIVACY PREFERENCES THEY HAVE CHOSEN TO BE INFORMED WHICH WHENEVER DEVICE INFORMATION OR CORE LOCATION INFORMATION IS TRANSMITTED BUT NOT DAYTIME INFORMATION, CORRESPONDINGLY AT POINT C-3, IT LET THE USER KNOW THAT THIS INVOLVES DEVICE DATA INFORMATION, SIMILARLY POINT C5 IN THE CODE REPRESENTS HOW IOT WATCH UNEMPLOYMENTS INFORMING THE USER PRIVACY VIOLATION DURING THE INFO BEING SENT TO AN UNAUTHORIZED HARD CODED RECIPIENT.

ONCE THOSE SOURCE CODE HAS BEEN INSTRUMENTED AND THE USER CONFIGURES PRIVACY PREFERENCES, THE USER INSTALLS THE INSTRUMENTED AP TO THE DEVICE, TRANSMITS DATA TO THE IOT WATCH SERVER WHENEVER SPECIAL DATA CODE IS FLAGGED THIS PERMITS IT TO IDENTIFY THE TYPE OF SENSITIVE INFORMATION AND COMBINED THIS WITH OTHER AP DATA LIKE THE DESCRIPTION TO UNCOVER LIKE, IT AS API TO SECURELY EXCHANGE THE DATA BETWEEN THE WATCH AND THE ANALYSIS SERVER.

IT CLASSIFIES THE CONTENTS OF SOMETHING CALLED ACCORDING TO FOUR, DEVICE INFO, DATES, TIME, LOCATION AND USER BEHAVIOR.

THESE LABELS WERE CHOSEN BASED ON OUR SURVEY RESULT AND A GIVEN STRING COULD BE ASSIGNED MULTIPLE PRIVACY LABELS DEPENDING ON THE SPECIFIC INFORMATION IT CONVEYS LIKE THE STRING THE DOOR WILL REMAIN OPEN FOR ANOTHER FIVE MINUTES.

NEXT SLIDE.
THE CLASSIFICATION OF SINGLY HOLE CONTENT IN IOT WATCH ACHIEVED THROUGH NATURAL LANGUAGE PROCESS OR NLP, A MACHINE LEARNING TECHNIQUE TO EFFECTIVE AND, TO BUILD THE MODEL WE COLLECTED THE THING CALLED CONTENTS OF 380 DIFFERENT APS FROM THE SAMSUNG SMART PHONE MARKETPLACE, FILTERED OUT PUNCTUATION OR STRAIN YOU DON'T SAY WORDS AND MANUALLY LABELED EACH ONE AS BELONGING TO THE FOUR DIFFERENT PRIVACY LABELS BUILT A CLASSIFIER USING SEVERAL NLP FRAME WORKS, 80% OF THE APS WERE USED AND THE REMAINING 20% WERE USED.
OVERALL OUR CLASSIFIER COULD ACHIEVE 94.3% ACCURACY WITH CLASSIFYING PRIVACY LABELS.
WE COLLECTED A TOTAL OF 540 SAMSUNG APS, 380 WERE USED TO DEVELOP OUR NLP MODEL I EXPLAINED AND REMAINING 160 OF THESE APS WERE USED TO EVALUATE THE PERFORMANCE, 120 WERE TAKEN DIRECTLY FROM THE SAMSUNG MARKETPLACE AND THE REMAINING 40 WERE FROM A MALICIOUS APS FROM THE IOT REPOSITORY AND SPECIFIC CORPUS USED TO EVALUATE SYSTEMS FOR IOT PRIVACY AND SECURITY, HE FIRST TESTED TO CLASSIFY INTO THE FOUR PRIVACY LABELS THE RESULTS OF WHICH CAN BE SEE HERE AT THE TABLE IN THE TOP RIGHT.
IT CONVERTED STRINGS IN THE PRIVACY LABELS WITH AN AVERAGE OF 93.8% ACCURACY AND 97.30% SPECIFICITY WE RESERVED THE HIGHEST FOR THE DAYTIME IN THE CATEGORIES LIKELY BECAUSE THESE

ARE THE MOST OBVIOUS TYPES TO IDENTIFY.
NEXT.
WE EVALUATED THE ABILITY TO DACA LIKES WE SPLIT THE LIKES WE WERE TESTING INTO LIKES VIA INTERNET LINKS AND MESSAGING WE FOUND IT WAS 100% EFFECTIVE AT IDENTIFYING SENSITIVE DATA VIA INTERNET SINGS FOR BOTH THE MARKET AND APS AND MALICIOUS, FOR MESSAGING IT WAS 100% EFFECTIVE ONLY THE MALICIOUS APS CONTAIN DAILY MESSAGING.
IN CONCLUSION, WE DEVELOPED A PRIVACY ANALYSIS TOOL IOTWATCH TO PERFORM SOURCE CODE ANALYSIS AND INSTRUMENT.
IT IDENTIFIED 100% EFFECTIVE, WAS ABLE TO CLASSIFY PRIVACY RELATED DATA WITH 94.25% ACCURACY.
ABLE TO ACHIEVE ALL OF THIS ADDING AN AVERAGE OF OVERALL, WE HOPE THAT OUR SUCCESS WITH IOTWATCH DEMONSTRATES IT'S POSSIBLE TO.
WE LEARNED USERS HAVE STRONG DESIRES FOR MORE TRANSPARENCY AND CONTROL OVER THE PRIVACY SENSITIVE INFORMATION IN IOT APS AND IOT WATCH IS PROOF THAT THESE DESIRES CAN BE MET.
WHY IT'S THE FIRST DYNAMIC ANALYSIS TO ACHIEVE THIS TO OUR KNOWLEDGE, HOPEFULLY IT'S FIRST GOOD STEP SUCH AS BECOMING WIDELY AVAILABLE AND EXPECTED BY IOTS IN THE FUTURE.
SO THANK YOU SO MUCH FOR TIME.
I JUST WANTED TO THANK MY PROFESSOR AND THE MAIN AUTHOR OF THIS PAPER, AS WELL AS THE NATIONAL SCIENCE FOUNDATION FOR

SUPPORTING THIS RESEARCH.
ALSO, I APOLOGIZE IF MY
CONNECTION WAS UNSTABLE.
STARTED RAINING HARD.
THANK YOU SO MUCH.
>> THANK YOU, GENEVIEVE.
YOUR CONNECTION WAS GREAT.
>> REMINDER WATCHING EUDIENCE IF
YOU HAVE QUESTIONS, PLEASE
E-MAIL THE QUESTIONS TO PRIVACY
CON AT FTC.GOV.
I WANTED TO OPEN UP THE
DISCUSSION TO PANELISTS, I THINK
IT'S INTERESTING THAT ONE OF THE
THEMES EMERGED IS A DESIRE FOR
MORE TRANSPARENCY, AND A TWO OF
THE TOOLS WERE DISCUSSED ARE
DESIGNED TO PROVIDE THAT GREATER
TRANSPARENCY.
WHAT IS HAPPENING TO OUR DATA?
SO MY FIRST QUESTION IS FOR
JENNIFER AND GENEVIEVE AND
SKILLED DETECTIVE IOT WATCH
TOOL.
ARE THEY STILL IN DEVELOPMENT DO
YOU HAVE PLANS TO MAKE THEM
AVAILABLE TO RESEARCHERS OR
OTHERS?
MAYBE START WITH JEFFREY.
>>> YES, THE SOURCE CODE IS
STILL IN DEVELOPMENT.
BUT OUR PAPER IS CURRENTLY IN
EVALUATION.
ONCE THE PAPER GETS PUBLISHED,
WE WILL BE PUBLISHING THE SOURCE
CODE TO MAKE AVAILABLE
PUBLICALLY TO ANYBODY HE DON'T
WANTS TO USE IT.
WE'RE GETTING EVERYTHING
TOGETHER NOW AND WE HAVE A GOOD
REPOSITORY SET UP, SO EVERYTHING
SHOULD BE AVAILABLE TO THE
COMMUNITY.
>> GENEVIEVE, WHAT ABOUT

IOTWATCH.
>> JEFF I DID WANT TO ASK A FOLLOW-UP QUESTION ON YOUR PRESENTATION.
CAN YOU SPEAK A LITTLE BIT MORE ABOUT SOME OF THE EFFECTS YOUR WORK HAS HAD SO FAR ON THE VOICE PERSONAL ASSISTANCE LIKE ALEXA AND GOOGLE HOME?
>> SURE.
WELL, LIKE I SAID IN THE PRESENTATION THAT GOOGLE DID TAKE DOWN SOME OF THE ACTIONS THAT WE HAD REPORTED.
BUT WE HAVE -- WE HAVE SPOKEN WITH AMAZON AS WELL, AND BUT THEY -- WE HAVE NOT BEEN ABLE TO REALLY SHOW THAT ANY ACTION HAS BEEN TAKEN AS OF RIGHT NOW.
BUT WE ARE IN COMMUNICATION WITH AMAZON, AND WE'RE TALKING WITH ONE OF THE DEVELOPERS THERE WHO'S IN CHARGE OF THE ALEXA PLATFORM.
AND SO WE'RE HOPING THAT YOU KNOW, SOME OF OUR WORK MAY LEAD TO SOME CHANGES OR SOMETHING ALONG THOSE LINES LATER ON DOWN THE LINE, BUT RIGHT NOW, WE'RE JUST, WE'RE NOT REALLY SURE, BECAUSE THEY, FOR AWHILE, WE CONTACTED THEM, AND WENT REALLY HEAR VERY MUCH BACK AND ALL OF A SUDDEN, WE KIND OF STARTED TALKING AND THEN NOW WE'RE BACK INTO THAT STAGE WHERE WE'RE NOT HEARING VERY MUCH BACK AGAIN.
SO.
>> DO YOU KNOW IF THE SKILL SET YOU IDENTIFIED TO THEM AS CONTAINING POLICY VIOLATIONS ARE STILL ACTIVE
>> YES, QUITE A FEW STILL ACTIVE.

WE'VE NOT TESTED ALL OF THEM BUT PLANNING TO GO BACK THROUGH AND TEST EVERYTHING AGAIN.
ALSO WE HAVE AN UPDATED VERSION OF OUR SYSTEM, SO WE'RE MAKING THE SYSTEM SMARTER, AND CAN ANALYZE DEEPER AND DEEPER INTO EACH SKILL.
IT'S NOT A VERY EASY TASK TO TALK BACK AND FORTH, YOU HAVE TWO COMPUTERS BASICALLY TALK TO EACH OTHER, BUT WE'RE PLANNING ON GOING BACK THROUGH AND DOING IT OVER AGAIN AND KEEPING A DATABASE OF THE INTERACTION MODELS BETWEEN EACH SKILL TO SEE HOW SKILLS CHANGE OVER TIME.
THAT'S ONE OF THE DETAILS TOO ABOUT HAVING THIRD PARTY DEVELOPERS AND SOURCE CODE ON THE BACK END, IS THAT SKILLS CAN BE UPDATED.
AND THEY DO NOT HAVE TO GO BACK THROUGH A VETTING PROCESS FOR THAT UPDATE.
AND SO WE HAVE -- WE CAN ONLY SEE THE SKILLS HOW THE SKILLS INTERACT WITH WHAT THE SKILL DOES.
AND SO WE'RE PLANNING ON KEEPING TRACK OF THAT IN DEVELOPING A DATA SET DOWN THE LINE.
>> YOU I THOUGHT YOU WOULD PROBABLY BE INTERESTED IN JEFFREY'S PAPER GIVEN YOUR RESEARCH AND A LITTLE BIT OF THE OVERLAP ON SOME PRIVACY ISSUES DESCRIBED.
YOU GAVE HELPFUL OBSERVATIONS OR SUGGESTIONS AT THE END OF YOUR PRESENTATION ABOUT WAYS THAT AMAZON COULD BETTER PROTECT ITS USER'S PRIVACY.
DID YOU WANT TO -- DID YOU HAVE

ANY ADDITIONAL THOUGHTS ABOUT
THAT ESPECIALLY IN LIGHT OF WHAT
YOU HEARD FROM JEFFREY
>> NO.
THAT'S A GOOD QUESTION,
ACTUALLY.
SO WE ACTUALLY ALSO HAD
INTERACTIVE WHEN WE FOUND SOME
FLAWS AND SO KIND OF
COMMUNICATION WITH THEM,
EXCHANGES AT THE BEGINNING AND
THEN SUDDENLY -- BUT WE DID TALK
ABOUT -- HAVE A LONG
CONVERSATION ABOUT ONE-HOUR
MEETING ABOUT SOME FINDINGS AND
OUR RECOMMENDATIONS AND THERE
WERE KIND OF INTERESTED IN
LOOKING AT THOSE RECOMMENDATIONS
BUT I THINK ONE OF THE THINGS
THEY'RE STILL LOOKING FOR IS
WHAT THE RECOMMENDATIONS REALLY
WERE AND SO THIS IS WHERE I
THINK WE NEED TO DO A LITTLE BIT
MORE RESEARCH IN TERMS OF WHAT
RECOMMENDATIONS WE'RE MAKING AND
WHETHER THAT'S REALLY IMPACTING
THE USERS AND MAKING THE RIGHT
CHOICES MAKING THEM AWARE ABOUT
SOME OF THE GAPS THAT MIGHT
EXIST.
SO I THINK WE'RE CURRENTLY
FOCUSING ON SOME USER STUDY ALSO
AND I THINK IT WOULD BE GREAT
ONCE WE'VE CONDUCTED SOME OF
THIS RESEARCH AND GO BACK TO
THEM SAYING OK -- THIS THING
REALLY WORKS, AT THAT STATE WE
WERE JUST MAKING RECOMMENDATIONS
WITHOUT ANY PROOF IN THAT
CONTEXT, SO I THINK THAT WOULD
BE THE BEST WAY TO GET THE BALL
ROLLING AGAIN WITH THEM SOME OF
THE PROCEDURALS
>> DO YOU HAVE SUGGESTIONS FOR

HOW CONSUMERS, THE USERS OF THE VOICE ASSISTANCE CAN BE MORE VIGILANT ABOUT PRIVACY WITH THE VOICE BASED SKILLS
>> YES, FROM A USER'S POINT OF VIEW, WHETHER THE SYSTEM SUPPORTS ANY ADDITIONAL, OR INDICATORS I THINK FROM A USER'S PERSPECTIVE, THERE'S CERTAIN THINGS WE CAN ALWAYS ADOPT.
AND SOME OF THE THINGS IS BASICALLY IS THAT THE LABELS WHICH I THINK (INAUDIBLE) WE TRIED THAT OURSELVES AND MANY TIMES, USERS REALLY GET IT WRONG AND THEY'VE DONE WHAT THEY THINK WILL ACTIVATE AND WHAT REALLY ACTIVATED.
SO ONE THING I WOULD SUGGEST IS THAT IF YOU DO INTERACT WITH THE SKILLS THEN YOU SEE SUDDENLY, SKILLS BEING INSTALLED OR ACTIVATED IN YOUR ACCOUNT, DO GO BACK AND SO HE WHAT'S ACTIVATED NOW AND SEE WHETHER THAT ACTUALLY MATCHES WHAT YOU REALLY WANTED TO INSTALL.
AND THE OTHER SUGGESTION WOULD BE THAT IF AT ANY POINT IN THE INTERACTION YOU FEEL LIKE THE SKILL IS ASKING FOR SOMETHING THAT DOESN'T MAKE SENSE, WITH THE FUNCTIONALITY, ASKING FOR PHONE NUMBER, LOCATION, ZIP CODE, THAT'S ANOTHER GREAT POINT TO STALL AND KIND OF RE THINK WHY IS THIS SKILL REQUIRING THIS INFORMATION, BECAUSE THERE ARE MANY OTHER ALTERNATIVE SKILLS OUT THERE WHICH MIGHT NOT ASK FOR THIS INFORMATION BUT YOU MIGHT STILL GET THE SAME SERVICES.
THAT'S ANOTHER THING END USER

YOU CAN DO.
AND THE LAST THING IS THAT BASICALLY, A LOT OF TIMES WE INTERACT WITH SKILL OR ACTIVATE SKILL FOR ONE AND THIS KIND OF TENDENCY HAPPENS IN THE LABS WE INSTALL APS FOR FUN NEVER USE THEM IN LONG-TERM.
SO I THINK IF YOU CHECK UP IS SOMETHING WE CAN KIND OF GET OURSELVES USED TO, SAYING THAT, OK, IN A MONTH LET ME SEE WHAT SKILL ACTIVATED ON MY ACCOUNT.
DO I REALLY USE ALL OF THEM IN A FREQUENTLY IF NOT, THEN THIS IS ANOTHER POINT PROBABLY WANT TO DEACTIVATE OR DELABEL THAT SKILL.
I THINK THESE ARE SOME OF THE PRACTICES OR GUIDELINES THAT WE, AS A CONSUMER CAN FOLLOW.
AND I THINK THOSE WILL DEFINITELY HELP IN KIND OF REDUCING THE RISKS TO SOME EXTENT.
>> I NOTICED THAT YOU WERE NODDING IN AGREEMENT TO ANUPAM'S AND HIS RECOMMENDATIONS TO USERS, I WAS WONDERING IF GIVEN YOUR STUDY, RELATED TO YOUR PRIVACY LABEL AND YOUR RESEARCH ABOUT CONSUMERS RISK PERCEPTIONS IF YOU HAVE THOUGHTS ABOUT USERS CAN PROTECT THEMSELVES AND IN PARTICULAR, YOU KNOW, EDUCATE THEMSELVES ABOUT THOSE PERCEPTIONS RISK PERCEPTIONS.
>> YES.
THAT'S A GREAT QUESTION, AND I THINK BASICALLY I JUST REALLY DON'T WANT TO PUT A LOT OF BLAME ON THE CONSUMERS HERE.
I THINK THE PROJECTS WE'RE CONDUCTING FOR IOT LABELING IS

THE IDEA HERE IS MANUFACTURERS SHOULD DISCLOSE WHAT THEY'RE DOING AND IT'S ON USERS TO READ THAT INFORMATION, IF IT'S FOR EXAMPLE IN A USABLE FORMAT WE KNOW THAT PRIVACY POLICIES PEOPLE ARE FOR THE REALLY READING THEM.
PEOPLE SHOULD EDUCATE THEMSELVES.
THEMSELVES, HOWEVER THIS INFORMATION SHOULD BE AVAILABLE.
THIS IS, WHERE WE SEE THIS HUGE GAP WE WOULD LIKE MANUFACTURERS TO TELL CONSUMERS IN AN UNDERSTANDABLE LANGUAGE WHAT THEY'RE DOING, AND HOW THEY'RE PROTECTING THEM, AND BASICALLY ALL THEIR PRIVACY PRACTICES THAT ARE RELEVANT TO CONSUMERS, CONSUMERS DATA.
I THINK IF THAT INFORMATION IS AVAILABLE, YES.
THEY NEED TO READ THAT INFORMATION, CONSUMERS NEED TO EDUCATE THEMSELVES IF THIS SOMETHING QUESTIONABLE TO THEM, THEY HAVE TO, FOR EXAMPLE, MAYBE CONTACT THE MANUFACTURER OR CONTACT PRIVACY SECURITY EXPERTS IF THEY KNOW THEM OR SOME HOW RAISE THAT CONCERN SO OTHERS WHO ARE MORE EXPERT IN THIS ISSUE CAN REALLY HELP THEM OR AT LEAST HELP THEM PROTECT THEMSELVES IF THEY CANNOT MAKE IT BETTER OR ANYTHING HELP CONSUMERS PROTECT THEMSELVES.
>> PART OF YOUR RESEARCH, DID YOU FIND INSTANCES WHERE RISK PERCEPTION WAS NOT ALIGNED WITH THE CONSUMER'S WILLINGNESS TO PURCHASE THE PRODUCT
>> YES.

GREAT QUESTION.
SO YES, SO AS YOU SAID BASIC ASSESS BOTH RISK PERCEPTION AND WILLINGNESS TO PURCHASE, IN MANY CASE THESE TWO WERE ALIKE, WHICH BASICALLY I THINK MAKES SENSE, BUT A FEW EXCEPTIONS, FOR EXAMPLE, CONSUMERS UNDERSTOOD THE RISK BUT THAT RISK WAS NOT ENOUGH FOR THEM TO CHANGE THEIR DESIRE TO PURCHASE THE DEVICE.
FOR EXAMPLE, ABOUT MULTI-FACTOR AUTHENTICATION PEOPLE KNEW THIS WOULD DECREASE THE RISK.
AND THEY PERCEIVED MORE RISK THAN THE DEVICE HAD, FOR EXAMPLE, MULTI-FACTOR AUTHENTICATION BUT TOLD US THAT THIS INFORMATION IS NOT GOING TO BASICALLY HELP THE PURCHASE THE DEVICE AND IN SOME CASES PARTICIPANTS WILL NOT PURCHASE THE DEVICE BECAUSE OF MULTI-FACTOR AUTHENTICATION BEFORE A OF USE ABILITY CHALLENGES, ANOTHER EXAMPLE WAS ABOUT SUPER TUESDAY UPDATE.
PEOPLE KNEW THAT AUTOMATIC UPDATE IS BETTER THAN OR MANUAL UPDATES IN TERMS OF RISK.
HOWEVER, THEY SAID THAT THEY STILL WOULD LIKE TO HAVE CONTROL OVER THE UPDATES.
THEY STILL PREFER MANUAL UPDATES OVER AUTOMATIC UPDATES.
I BELIEVE IT SHOWS THAT RISK IS NOT ENOUGH.
LABEL SHOULD NOT JUST BE DESIGNED JUST TO COMMUNICATING THE RISK AND THAT'S IT.
THE PRACTICE SHOULD BE THE USE.
SO THAT NOT ONLY CONVEYS A RISK FOR THE ONLY DECREASE THE RISK, BUT ALSO THERE ARE USABLE, SO

PEOPLE ARE INTERESTED IN USING
THEM AND ARE BASICALLY GOING TO
PURCHASE THE DEVICE BECAUSE OF
THOSE FEATURES, NOT GOING TO
TURN AWAY BECAUSE OF THE USE
ABILITY ISSUES.
>> INTERESTING YOUR PAPER
REPORTED SELF-REPORTING PURCHASE
BEHAVIOR FOR CONSUMERS AND
THERE'S ALSO A LOT OF DEBATE
ABOUT WHAT PEOPLE SAY AND DO, AS
RELATES TO PRIVACY.
DO YOU HAVE THOUGHTS OR
EXPECTATIONS ON HOW YOUR IOT
LABEL COULD IMPACT REAL
PURCHASING BEHAVIOR?
>> GREAT QUESTION.
SO I THINK THE MAIN REASON THAT
WE DID STUDIES LIKE THIS LINE
STUDY IN SELF REPORTED FASHION
WAS THAT THESE DO NOT HAVE THE
LABELS, THEY CANNOT HAVE LABELS
IN -- IN REAL PURCHASE BEHAVIOR,
BECAUSE DEVICES DO NOT HAVE
LABELS BASICALLY.
WE CANNOT ONLY TEST THAT IN REAL
LEVICK PURCHASE BEHAVIOR.
BUT IF YOU LOOK INTO OTHER
LITERATURE, FOR EXAMPLE, FOOD
LITERATURE, WE KNOW THAT
CONSUMERS WHO ARE MORE
INTERESTED IN HAVING BETTER
HEALTH, FOR EXAMPLE, THOSE ARE
THE ONES WHO WOULD LOOK INTO
NUTRITION LABELS OR THOSE WHO
HAVE MORE KNOWLEDGE WOULD LOOK
INTO NUTRITION LABELS, SO
THERE'S DIFFERENT FACTORS THAT
MIGHT IMPACT ON YOU INTERESTED
YOU WOULD BE IN LOOKING FOR THAT
INFORMATION AND HOW THAT
INFORMATION WOULD IMPACT YOUR
PREFERENCES AND DESIRE TO
PURCHASE FOR EXAMPLE THE DEVICE,

SUCH AS INTEREST, SUCH AS KNOWLEDGE, SO WE DON'T REALLY KNOW FOR SURE HE DON'T LABELING IS GOING TO IMPACT REAL PURCHASE BEHAVIOR BUT BASED ON WHAT WE HEARD FROM THE CONSUMERS, IN ALL THIS STUDIES CONDUCTED WE KNOW THAT THE LABEL IS UNDERSTANDABLE TO THEM.
BUT WE DON'T KNOW WHETHER THAT WOULD CHANGE THEIR WILLINGNESS TO PURCHASE IF BEING PRESENTED THE ACTUAL PURCHASE BEHAVIOR.
>> GENEVIEVE I'M GLAD YOU WORKED OUT THE CONNECTION PROBLEMS. WELCOME BACK.
I WANTED TO GO BACK TO THE QUESTION BEFORE YOU DROPPED OFF ABOUT WHETHER OR NOT THE IOT WATCH TOOL WAS STILL IN DEVELOPMENT AND IF THERE'S PLANS TO MAKE IT AVAILABLE TO RESEARCHERS OR OTHERS.
>> SO IOT WATCH IS ONLY FOR SMART PHONES PLATFORM BUT WE WOULD LIKE TO MAKE THE TOOL PUBLICALLY AVAILABLE DOWN THE LINE AND POLICEMEN TO OTHER PLATFORMS LIKE OPEN HABIT AS WELL FOLLOWING A COMPLETE, AT PRESENT WE HAVE A DEMO VERSION OF THE IOTWATCH AVAILABLE.
THAT CAN BE FOUND.
AND THIS DEMO ALLOWS USERS TO INPUT THE IOT SOURCE CODE AND RETURNS AFTER HAVING CALLS AND INSTRUMENTED.
AND SO THAT INSTRUMENTED SOURCE CODE WON'T BE ABLE TO BE USED BY ANYTHING BECAUSE THE PORTION OF THE IOT THE ANALYZER IN PUBLICALLY AVAILABLE YET.
BUT THAT'S AVAILABLE TO PEOPLE CAN TRY IT OUT AND SEE WHAT IT

WOULD DO.
>> I UNDERSTAND -- CORRECT ME IF I'M WRONG -- THAT THE WAY IOT WATCH WORKS SENDS DATA TO SERVERS FOR IT'S ANALYSIS.
ARE THERE MEASURES IN PLACE THAT PROTECTS THE DATA?
>> YES, IOT WATCH USES TLS, IOTWATCH DOESN'T COLLECT ANY IN ADDITION TO THE INFORMATION THAT'S ALREADY INCLUDED IN THE STRINGS SENT IT TO FROM THE AP.
ALSO, OUR TOOLS DON'T FINGERPRINT OR EXPOSE ANY OF USER ACTIVITY IS WHAT SO EVER, BECAUSE IT DOESN'T ACTUALLY COLLECT INFORMATION AND STORE IT.
IT SENDS THE INFORMATION, ANALYZES RESPONDS RIGHT BACK.
AND AS PART OF IOTWATCH WE INCLUDED TUTORIAL THAT EXPLAINS TO THE USER WHAT WE DO WITH THE INFORMATION AND THAT CAN BE FOUND IN THE PAPER AS WELL.
ON THE.
>>> IF A DEVELOPER USES ENCRYPTION, WOULD THAT RE HAVE ANIED.
>> THE WAY IOT WORKS NOW, IT DOESN'T ACCOUNT FOR ENCRYPTION, BUT IF AN AP WERE TO BE FOUND ENCRYPTED THERE ARE WAYS AROUND THIS, IOT WORKS BY EXTRACTING IOT STRINGS FIVE MINUTES IN THE IOT APS AND IN THE CASE OF AN AP IMPLEMENTING ENCRYPTION, THE AP WOULD SAY NEED TO IMPLEMENT BEFORE SENDING THE KIMAX, AND THEREFORE, IOT ANALYSIS COULD BE EASILY MODIFIED TO EXTRACT THE AP INFORMATION BEFORE THE ENCRYPTION IN PLAIN TEXT TO VIRTUAL ANYWAY.

HOWEVER, WE FOUND HAD THAT'S ACTUALLY A MOOT POINT FROM WHAT WE'VE SEEN SO FAR, BECAUSE OUT OF THE 540 SMART THINGS ASKED THAT WE LOOKED AT.
A LOT OF APS IN CREPTED THE IOT RATHER THAN JUST THE TLS.
IF WE HAD HAD ENCOUNTERED AN AP ENCRYPTING DATA THAT IN ITSELF WOULD HAVE FLAGGED IT TO US.
>> SORT OF INTERESTED IN THE THOUGHTS OF EVERYBODY ON THE PANEL ABOUT FUTURE AREAS OF RESEARCH REGARDING IOT THAT YOU THINK WOULD BE PARTICULARLY USE USEFUL.
>> I DEFINITELY THINK THAT SORT OF TO ECHO WHAT I HEARD SAYING I THINK ONE OF THE BIGGEST AREAS OF RESEARCH ARE DEVELOPMENT IN GENERAL AS IOT NEEDS TO BE SOME SORT OF REGULATION FOR DESCRIBING THE PRIVACY IMPACTS OF IOT DEVICES TO CONSUMERS.
I THINK THAT IT'S SOMETHING LIKE THAT WAS IN PLACE, WE WOULDN'T HAVE HAD TO LIKE IOT WATCH WOULDN'T BE NECESSARY BECAUSE THE APS WOULD BE EXPOSING WHAT THEY DO WITH PRIVATE INFORMATION THEMSELVES.
AND SO I THINK THAT IN TERMS OF LIKE FUTURE RESEARCH, WE NEED TO JUST BE LOOKING AT BETTER WAYS OF ANALYSIS MAYBE MORE DYNAMIC ANALYSIS TOOLS AS WELL AS STATIC ANALYSIS JUST TO ANALYZE HOW APS ARE RUNNING AND WHAT THEY DO WITH THE INFORMATION NOT ONLY THAT USERS PUT IN BUT ALSO THE INFORMATION THAT THE APS THEMSELVES ARE DEALING WITH JUST IN TERMS OF LIKE WHETHER A DOOR IS OPEN OR THINGS LIKE THAT.

>> PARDIS?
>> SO I THINK WHAT I FEEL IS MISSING HERE IS REALLY THE REALISTIC PURCHASE SETTINGS AND REALLY UNDERSTANDINGS THAT THEIR CONSUMERS WOULD UNDERSTAND PRIVACY AND SAFETY INFORMATION THAN PURCHASING DEVICES AT THE TIME OF PURCHASE AT THE POINT OF SALE.
AND I THINK IN OTHER COUNTRIES, FOR EXAMPLE, IN FINLAND AND SINGAPORE, THEY ALREADY HAVE IOT LABELS, WE DON'T HAVE THAT IN THE U.S. FOR SURE BUT I THINK IF MANUFACTURERS ARE FOR EXAMPLE GOING TO ADOPT A LABEL, MAYBE GOING TO JUST BE IN A PILOT STUDY TO JUST ADOPT A LABEL AND THEN WE CAN STUDY THEM AND SEE WHEN THEIR CONSUMERS ARE UNDERSTANDING THIS INFORMATION, THEY UNDERSTAND THE RISK, AND THINGS LIKE THAT, I THINK THIS IS REALLY IMPORTANT HERE, BECAUSE THIS CAN PUSH THIS EFFORT FORWARD A LOT BECAUSE IT CANNOT JUST CONTINUE WORKING ON SELF REPORTED RESPONSES WE REALLY WANT TO UNDERSTAND THE REALISTIC BEHAVIOR AND I THINK THE NEW WHITE HOUSE EXECUTIVE ORDER TO WORK TOGETHER TO BASICALLY CONDUCT A PILOT AND LOOK INTO THE EFFORTS INTO LABELINGS SMART DEVICES I THINK THIS IS NOW GAINING SOME INTEREST IN THE U.S.
AND I'M ACTUALLY OPTIMISTIC ABOUT THIS THIS BASICALLY U.S. IS ALSO GOING TO LOOK INTO THIS AND MAYBE IN THE NEAR FUTURE, WE'RE GOING TO HAVE THIS LABELS FOR DEVICES AND THEN WHOLE NEW

SET OF NEW RESEARCH STUDIES WILL BE CONDUCTED AFTER WE HAVE THOSE LABELS.
>> ANUPAM?
>> SO FOR THE CONTEXT OF INTERFACES I THINK ONE OF THE FEW INTERESTING RESEARCH QUESTION IS GOING TO BE HOW DO WE DESIGN EFFECTIVE INDICATORS OR INTERVENTIONS FOR VOICE INTERFACE, IN MANY WAYS, WHEN USERS ARE INTERACTING WITH VOICE INTERFACES THEY TYPICALLY THINK WHOEVER IS, THAT'S THE COMPANY THAT DOING ALL THE WORK.
BUT WHEN YOU OPEN UP THIRD PARTIES THAT BECOMES MORE TRICKY.
I THINK DESIGNING EFFECTIVE INDICATORS OR VOICE WITH INTERVENTIONS I THINK THAT IS GOING TO BE CHALLENGING AND ALSO GOING TO BE INTERESTING BECAUSE WE NEED THAT AS USERS WE KNOW AT SOME POINT ARE NOT ALWAYS CALLING OUT TO CHECK ALL OF THE INFORMATION BY THEMSELVES, SO WE NEED TO PLACE INTERVENTIONS OR INDICATORS AS MUCH AS POSSIBLE THROUGHOUT THEIR INTERACTION THROUGH THE VARIOUS PLATFORMS AND I THINK THAT'S GOING TO BE A RESEARCH PROBLEM THAT WE'LL SEE IN THE VERY NEAR FUTURE.
>> WHAT ABOUT YOU JEFFREY, WHAT ARE YOUR THOUGHTS?
>> WELL, ONE OF THE THINGS I THINK WE'VE FOUND OVER TESTING THUS FAR IS THAT ACTUALLY DEVELOPERS A LOT OF TIMES WE DON'T BELIEVE THEY UNDERSTAND THAT THEY'RE ACTUALLY VIOLATING POLICIES, THEY'RE JUST DEVELOPING CODE IN A BEDROOM OR

SOMETHING ON THOSE LINES.
AND SO I COULD DEFINITELY SEE
SOME OF OUR FUTURE RESEARCH
ACTUALLY IS IN THE FIELD OF
BEING ABLE TO TEST SOURCE CODE
BEFORE IT EVEN GOES TO THE TO
THE PLATFORM.
SO SOME SORT OF TOOL THAT YOU
CAN TEST YOUR OWN SOURCE CODE
FOR POLICY VIOLATIONS, THAT SORT
OF THING.
ALSO, DYNAMIC PERMISSION MODELS
BECAUSE IT'S VOICE ACTIVATED,
VOICE INTERACTION, IT'S VERY
DIFFICULT TO ASK PERMISSION SO
HOW CAN YOU DESIGN A PERMISSION
MODEL THAT'S ACCURATE THAT WOULD
ACTUALLY INFORM THE CONSUMER YOU
KNOW, DO YOU GIVE PERMISSION FOR
THIS PARTICULAR SKILL TO COLLECT
THIS PARTICULAR DATA AT THIS
PARTICULAR POINT?
AND THAT SORT OF QUESTION, THAT
IS GOING TO PROBABLY BE AN OPEN
QUESTION FOR AWHILE JUST BECAUSE
OF THE PLATFORM.
>> SO WE ARE ABOUT AT THE END OF
OUR TIME.
I WANT TO ENCOURAGE EVERYBODY TO
GO TO THE PRIVACY CON PAGE OF
FTC.GOV WHERE YOU CAN READ
PRESENTER'S FULL RESEARCH PAPERS
THEY'RE WELL WORTH YOUR TIME.
WE ARE NOW GOING TO TAKE A SHORT
BREAK PLEASE IS THAT CLEAR
AROUND FOR PANEL AND PRIVACY AND
TEAMS I WANT TO THANK OR
PANELISTS AND SHARING WITH US
TODAY.
AND THANK EVERYONE AT HOME
JOINING US.
THANK YOU EVERYONE.
§.
§ §

.
>>> OUR FURS ER IS MOHAMMAD MANNAN.
HE'LL BE PRESENTING ON HIS PAPERS TITLED ETRADE BY THE GUARDIAN, SECURITY AND PRIVACY RISKS OF PARENTAL CONTROL SECOND PAPER, PARENTAL CONTROLS.
SECOND WILL BE CAMERON GONNELLA FROM BBB NATIONAL PROGRAM, SHE'LL BE PRESENTING ON HER PAPER TITLED RISKY BUSINESS THE CURRENT STATE OF TEEN PRIVACY IN THE ANDROID MARKETPLACE, A QUESTION SECOND TO MAKE A CLARIFICATION, THE RESEARCH WE'LL BE DISCUSSING TODAY WAS CONDUCTED WHOLE UNTIL HOUSE BY BBB NATIONAL PROGRAM AND DID NOT INCLUDE OUTSIDE FUNDING.
AFTER EACH PRESENTATION, WE'LL HAVE A BRIEF Q AND A AND HOPEFULLY AT THE END FOR GROUP DISCUSSION, IF ANYONE IN THE AUDIENCE HAS QUESTIONS AS WE'RE MOVING ALONG, FEEL FREE TO E-MAIL THEM AT PRIVACY CON AT FTC.GOV AND WE CAN HOPEFULLY GET TO THEM.
TIME PERMITTING.
WITH THAT, WE HAVE A FANTASTIC PANEL AHEAD OF US, LET'S JUMP RIGHT IN AND MOHAMMAD WITH THAT, I'LL PASS IT TO YOU FOR YOUR PRESENTATION.
>> THANKS FOR THE INTRODUCTION.
HELLO AGAIN, MY NAME IS MOHAMMAD MANNAN.
I'M GOING TO PRESENT OUR WORK ON PARENT CONTROL SOLUTIONS.
THIS IS A JOINT WORK WITH MY COLLABORATORS HERE FROM CONCORD UNIVERSITY, CANADA, THIS WORK WAS PRESENTED AT EXIT LAST YEAR.

SLIDE TWO.
PARENTAL CONTROL SOLUTIONS ARE SCENE BY NECESSARY BY MANY PARENTS TO KEEP CHILDREN AND TEENS SAFE ONLINE, WHICH HAS BECOME A SIGNIFICANT ISSUE EVEN BEFORE THE COVID CATASTROPHE.
MANY PRODUCTS ARE ALSO TO HELP PARENTS IN THIS REGARD AND PRODUCTS COME WITH A LOT OF SAFETY PROMISES I'M QUOTING HERE ONE PRODUCT, WHICH CLAIMS THAT PARENTS DO NOT NEED TO WORRY AND GLANCE OVER THEIR CHILDREN'S SHOULDER AND THE PRODUCT WILL TAKE CONTROL OVER ALL INTERNET ACTIVITIES.
THESE PRODUCTS ARE REPRESENTED BY SOME TRUST GOVERNMENT SOURCES SUCH AS THE U.S. FTC AND CHILD INTERNET SAFETY.
SOLUTION BETWEEN CHILDREN'S DEVICES AND EXTERNAL DEVICES THE SOLUTION CAN BE AN AP OR AN APPLICATION IN A DEVICE OR SUITLAND A BROWSER ADD ON OR IMPLEMENTED IN A SEPARATE INDEPENDENT DEVICE.
THE SOLUTION WILL CHECK ALL ONGOING NETWORK CONNECTIONS AND IN SOME CASES MESSAGES.
AND ALLOW THE ONE DEEMED TO BE SAFE.
WE ANALYZED THE SOLUTIONS FROM MULTIPLE PLATFORMS INCLUDING ANDROID AND WINDOWS SYSTEMS, CHROME BROWSE ER ADD ONES AND INDEPENDENT NETWORK DEVICES WE DID IT FOR MULTIPLE PLATFORMS JUST SO WE CAN HAVE A COMPREHENSIVE VIEW OF THE DOMAIN FROM A SECURITY AND PRIVACY PERSPECTIVE.
SO TO ENABLE PARENTAL CONTROLLED

FUNCTIONS THE SOLUTION REQUIRE POWERFUL PRIVILEGES NETWORK DEVICES GENERALLY MONITOR ALL EXTERNAL DOMAINS AND TRAFFIC. BUT USUALLY THEY DON'T INTERCEPT THE TRAFFIC, WHICH IS DONE BY SOME WINDOWS APPLICATIONS AND CHROME ADD, ONES NEED TO SEE ALL BROWSER DATA.
FOR ANDROID APS, THEY REQUIRE INCLUDING DEVICE STEAKS, AND DEVICE MANAGEMENT AND SOME CASES SUPER USER PERMISSIONS.
SOME OF THEM ALSO REAR TO HAVE ACCESS TO MONITOR ALL USER ACTIONS ON DEVICE, WINDOW CONTENT FROM OTHER APPLICATIONS, PHONE CALLS, SMS MESSAGES AND REAL TIME LOCATION.
SOME REQUIRE AUTHENTICATION CREDENTIALS FOR OTHER SOCIAL MEDIA PLATFORMS LIKE FACEBOOK AND YOUTUBE TO MONITOR THE COMMENTS AND THE MESSAGES IN THOSE PLATFORMS.
BECAUSE THESE PLATFORMS, THESE SOLUTIONS ARE HIGHLY PRIVILEGED, AND THEY AL DEAL WITH CHILDREN'S DATA, WE WANTED TO KNOW IF THEY'RE SECURE ENOUGH TO PREVENT SIMPLE, AND IF THEY THEMSELVES VIOLATE USER PRIVACY BY COLLECTING UNNECESSARY PERSONAL DATA OR BY EXPOSING PERSONAL DATA TO THIRD PARTIES.
FOR THIS, WE DESIGNED AT THIS FRAMEWORK AND ANALYZED RELATIVE SOLUTIONS.
PLEASE SEE OUR PAPER IF YOU'RE INTERESTED IN THIS FRAMEWORK I'M NOT GOING TO DISCUSS MUCH HERE.
IN SUMMARY, WE CHECK THE SOLUTION CODE, TRAFFIC GENERATED BY THEM DURING USAGE, AND ALSO

THEIR ONLINE INTERFACES.
SLIDE SIX.
OUR RESULTS SOMEBODY FOR THESE SOLUTIONS ISN'T QUITE PRETTY.
AND 54 SOLUTIONS THAT WE TESTED, WE FOUND 172 PRIVACY AND SECURITY VULNERABILITIES, MOST IN ANDROID APS BUT SEVERAL NETWORK DEVICES FROM ADD, ONES AND WINDOWS APPLICATIONS ARE ALSO SIMILARLY VULNERABLE.
I'M NOT I'M GOING TO DISCUSS A WHOLE LOT OF THE RESULTS BUT I'LL PRESENT A FEW EXAMPLES VULNERABILITIES.
SLIDE SEVEN.
THE FIRST EXAMPLE I HAVE HERE IS AN IS THAT YOUR MECHANISM IN BLOCK SI NETWORK THE NETWORK CONTROLLED DEVICE.
IN THIS ONE, BLOCKS THE SERVICE AND UPDATED WEAR ALWAYS CREEP GRAPHIC OF THE BINARY FARM WEAR, ANYONE IN THE NETWORK CAN REPLACE THE FIRM WEAR AND HASH CODE WITH ANYTHING THEY'D LIKE INCLUDING MALWARE, BECAUSE IT DOES NOT REQUIRE ANY SECRET TO COMPUTE AND BINARY IS ALSO NOT SIGNED.
SLIDE EIGHT.
THE SECOND EXAMPLE I HAVE HERE IS AN ANDROID AP CALLED SECURITY TEEN SECURES CHILDREN'S ACTIVITIES ON THE CYBER SIDE AND ALLOWS PARENTS TO CHECK THE DATA AT THE LATER POINT IN TIME.
UNFORTUNATELY, THE PROVIDE AN API, YOU ONLY NEED APPARENTLY E-MAIL ADDRESS TO HAVE ACCESS TO THE PARENTAL ACCOUNT WITHOUT KNOWING THE ACCOUNT PASSWORD.
SLIDE NINE.
SOME OTHER NOTABLE FROM OUR

ANALYSIS INCLUDE THE FOLLOWING.
WE HAVE SEND 13 SOLUTION THAT ALLOW ILLEGITIMATE ACCESS TO SERVER STORED DATA SIMILAR TO THE EXAMPLE THAT I DISCUSSED IN THE PREVIOUS SLIDE.
AT SOLUTIONS SEND PERSONAL DATA OVER IN PLAIN TEXT AND 16 OTHERS, EVEN THOUGH THEY USE HTTPS THEY CAN BE EASILY DOWNGRADED TO STTP.
SIX OTHER SOLUTIONS ALLOW EASY WORK AND WE HAVE ANALYZED SOME SOLUTIONS CERTIFIED UNDER THE FTC APPROVED KID SAFE PROGRAM AND WE FOUND THEY USE THIRD PARTY TRACKERS AND IN SOME CASES ALSO EXPOSE PERSONAL DATA INCLUDING EVEN ACCOUNT CREDENTIALS.
SLIDE TEN.
DISCUSS SOME EXAMPLES OF WHAT IT CAN DO WITH VULNERABILITIES WE EXPOSED.
CONTROL OF A NETWORK DEVICE WILL OCCUR TO MONITOR ALL DEVICES AND ACTIVITIES AND USE THE PARENTAL CONTROL DEVICE IN OTHER MALICIOUS ATTACKS.
BY HAVING ACCESS TO THE PARENTAL ACCOUNT, THIS WILL BE QUITE DEVASTATING BECAUSE THIS MAY ENABLE FULL CONTROL OF THE CHILD DEVICE, IN THIS CASE, CAN INSTALL OR REMOVE IMPLICATIONS FROM THE DEVICE AND ALLOW OR BLOCK PHONE CALLS AND INTERNET CONNECTIONS AND EVEN ACCESS REAL-TIME LOCATION DATA FROM THE DEVICE.
THE UNPROTECTED SOFTWARE THAT WE HAVE FOUND FROM THEM CAN ACCESS THE DATA COLLECTED FROM OVER HALF MILLION USERS.

MOST OF WHO ARE TEENS AND CHILDREN.
THE USER STTP CAN ALLOW AN ATTACKER TO DROP OR MODIFY SOME VERY SENSITIVE MESSAGES LIKE AN SOS MESSAGE, WHICH IS SUPPOSED TO BE SENT WHEN THE CHILD IS IN ACTUAL DANGER.
OVERALL, MOST PARENT TALL CONTROL SOLUTIONS WE HAVE ANALYZED TO NOT MEET PRIVACY EXPECTATIONS AND INTRODUCE NEW VENUES AND MAKE USERS VULNERABLE.
AS THESE PRODUCTS ARE SEEN AS ESSENTIAL, PARENTS CANNOT SIMPLY DELETE THEM.
JUST LIKE A GAME OR OTHER UNESSENTIAL APPLICATIONS WHICH, IF YOU KNOW THAT THEY ARE NOT MEETING YOUR PRIVACY OR SECURITY EXPECTATIONS, YOU CAN SIMPLY GET RID OF THEM.
SO SUGGEST THAT THIS PRODUCT SHOULD BE DESIGNED IN WAY THAT EVEN IF THEY WON'T PROVIDE PERFECT FUNCTIONALITY, THEY SHOULD DO NO HARM IN TERMS OF PRIVACY AND SECURITY EXPOSURE.
AND IF AND WHEN THERE IS A BREACH, THE SOLUTION PROVIDERS MUST ACCEPT LIABILITIES FOR THOSE BREACHES AND ONLY STRICT REVELATIONS CAN BE MADE THAT HAPPEN.
SLIGHT 12.
R REGARDING VULNERABILITIES WE FOUND, WE CONTACTED ALL COMPANIES MULTIPLE TIMES AND STILL COULD NOT GET A RESPONSE FROM SOME.
FEW OF THEM FIXED THE PRODUCT BUT STILL MANY VULNERABILITIES REMAIN OPEN.

SEVERAL MONTHS AFTER WE FIRST CONTACTED THEM.
FINALLY I WANT HOPE CANNOT AFFORD THE SUPPORT IN THIS PROJECT.
I WANT TO THANK YOU ALL FOR YOUR TIME AND ATTENTION, I'LL BE HAPPY TO TAKE QUESTIONS.
YOU CAN E-MAIL ME AFTERWARDS IF YOU HAVE FURTHER QUESTIONS.
THANKS.
>>> THANK YOU, MOHAMMAD.
THAT WAS FANTASTIC.
THANK YOU FOR NOT ONLY THE PRESENTATION, BUT ALSO YOUR RESEARCH.
YOUR RESEARCH PROVIDES SOME REALLY INTERESTING FINDINGS ABOUT THE PARENT AL CONTROL SOLUTIONS MANY ARE QUITE SCARY ESPECIALLY FOR PARENTS.
DO YOU HAVE ADVICE ON WHAT PARENTS CAN DO TO SAFE AND EFFECTIVE PARENTAL CONTROL SYSTEM.
>> FOR PARENTS, YOU KNOW, I MEAN, I DON'T BELIEVE THAT MOST OF THEM ARE TECH SAVVY, SO IT WOULD BE DIFFICULT FOR THEM TO CHOOSE SOMETHING BY UNDERSTANDING THEIR SECURITY AND PRIVACY CONSEQUENCES.
OUR REPORT CAN HELP TO SOME EXTENT.
WE ALSO HAVE ACTUALLY A WEBSITE WITH DETAILS INFORMATION ON EACH PRODUCT BUT OF COURSE, YOU KNOW, WE ONLY ANALYZED SOME YOU KNOW, SELECTED SET OF PRODUCTS, NOT ALL PRODUCTS THAT ARE AVAILABLE IN THE MARKETPLACE.
SO GENERALLY WHAT I SUGGEST IS PARENTS SHOULD AVOID THE PRODUCTS THAT COME WITH SOME,

YOU KNOW, INVASIVE FEATURES
BECAUSE THOSE FEATURES, IF NOT
WILL PROTECT THEM, CAN SURELY
CAUSE SERIOUS ISSUES AND PARENTS
CAN ALSO CHECK HOW MUCH DATA IS
COLLECTED BY THE SOLUTIONS IN
THEIR OWN LINE ACCOUNT
INTERFACE, WHATEVER DATA THEY
MAY SEE THEY SHOULD CONSIDER
THAT THE CONSEQUENCE OF THAT
BEING LEAKED AT SOME POINT IN
THE FUTURE.
SO INSTEAD OF USING THIS THIRD
PARTY SOLUTIONS, WHAT I ALSO
SUGGEST TO USE PARENTAL CONTROL
FUNCTIONALITIES WHICH ARE NOW
BUILT INTO MOST OPERATING
SYSTEMS EVEN THOUGH THEY ARE NOT
FANCY, BUT THEY MAY BE
SUFFICIENT FOR MOST PARENTS.
>> THAT'S HELPFUL.
JUST AS A FOLLOW-UP TO THAT, YOU
MENTION THAT ONE OF THE THINGS
THAT PARENTS SHOULD AVOID ARE
SOLUTIONS WITH WHAT YOU CALL
INVASIVE FEATURES, WHAT A
INVASIVE FEATURES?
>> SO INVASIVE FEATURES ARE IF
THE SOLUTION CAN INSTALL OR
REMOVE ANY AP, IF IT CAN BLOCK
YOU KNOW, A PHONE CALLS OR SMS
MESSAGES OR INTERNET CONTENTS,
WHICH MAYBE YOU KNOW, IMPORTANT
FOR THE CHILD, AND IF THOSE
FEATURES ARE COMPROMISED THE
CHILD MAY BE HARM IN THE REAL
WORLD.
PARENTS SHOULD BE AWARE OF THESE
FEATURES, THAT WHENEVER YOU SEE
THAT THEY ARE TALKING ABOUT WE
CAN GIVE A LOT OF CONTROL TO YOU
AS A PARENT, THERE IS A DARK
SIDE OF THAT CONTROL THAT YOU
KNOW, IF THOSE FEATURES CAN

REALLY BACKFIRE AT SOME POINT.
>> THANK YOU, THAT'S REALLY HELPFUL.
SO YOU KNOW, IF WE LOOK ON THE OTHER SIDE OF THE COIN, PERHAPS WE SHOULDN'T PLACE ALL OF THE RESPONSIBILITIES ON THE PARENT.
I'M CURIOUS IF YOU HAVE ANY OPINIONS ON WHAT THE DEVELOPERS OF THESE PARENT AL CONTROL SOLUTIONS OR OR FOR EXAMPLE, GOOGLE AND APPLE, WHAT THEY CAN DO TO IMPROVE SOME ISSUES THAT YOU FOUND IN YOUR RESEARCH.
>> APPLE IN THE MARKETPLACE, THEY COMPETE WITH EACH OTHER. THEY WANT TO PROVIDE AS MANY FANCY FEATURES AS POSSIBLE WHETHER THOSE FEATURES ARE NECESSARY OR NOT, YOU KNOW, SO THEY JUST WANT TO PLAY MORE FEATURES, I THINK THEY SHOULD SEE IT MORE FROM THE OTHER SIDE OF IT.
IF WE USE THIS INVASIVE FEATURES IT CAN ACTUALLY CAUSE ISSUES FOR US IN THE FUTURE, SO THEY SHOULD AVOID USING POWERFUL PRIVILEGES IF THEY ARE NOT NECESSARILY FOR THE FUNCTIONALITY OF THEIR SOLUTION.
AND THEY CAN ALSO AVOID USING YOU KNOW, SOFTWARE THAT WILL OPEN KITS OR LIBRARIES THAT CONTAIN THIRD PARTY RECORDS, AND TO AVOID SIMPLE MISTAKES IN THE DESIGN AND IMPLEMENTATION, THEY CAN ALSO TRY OUT OUR DISK FRAMEWORK FOR THE MARKET PROVIDERS LIKE GOOGLE OR APPLE, WE KNOW THEY DO A LOT TO KEEP THE MARKETPLACE MALWARE FREE BUT I THINK THEY DON'T DO ENOUGH TO MAKE IT AS PRIVACY FRIENDLY,

ESPECIALLY THEY SHOULD REALLY CONSIDER HERE THAT YOU KNOW, CHILDREN'S SAFETY AND PRIVACY IS AT -- THEY SHOULD REALLY TAKE IT MORE SERIOUSLY.
AND THIS PROVIDERS TAKING REALISTIC APS FROM USING POWERFUL FEATURES LIKE DEVICE ADMINISTRATION OR MANAGEMENT THAT I MENTIONED BEFORE.
WHICH WERE DESIGNED FOR SOME OTHER PURPOSES, NOT FOR PARENTAL CONTROL PURPOSES, THEY CAN SIMPLY BLOCK THESE FEATURES, YOU KNOW, WHEN AN AP REALLY DON'T NEED TO USE THESE FEATURES.
>> THANK YOU, THAT WAS FANTASTIC.
AND NOW TURN OVER TO CAMERON FOR HER PRESENTATION.
>> AS YOU SAID I WILL BE PRESENTING FINDINGS FROM OUR WHITE PAPER STUDY RISKY BUSINESS THE CURRENT STATE OF TEEN PRIVACY IN THE MARKETPLACE, THIS WHITE PAPER STUDY WAS CONDUCTED BY MYSELF AND TEAM WITH THE EMPHASIS FOR A NEW PROGRAM WE'RE DEVELOPING CALLED THE TEENAGE PRIVACY PROGRAM AND THAT HAS THE GOAL OF ULTIMATELY CREATING A SET OF SELF REGULATORY FRAMEWORK AND STANDARDS FOR INDUSTRY BEST PRACTICES REGARDING TEEN PRIVACY ONLINE.
IF YOU HAVE QUESTIONS OR WOULD LIKE TO KNOW MORE I WILL HAVE CONTACT INFORMATION AT THE END OF MY PRESENTATION.
SO AWAY DO WE FOCUS ON TEENAGERS
>> WE FOCUS FOR TWO REASONS FIRST AS YOU CAN SEE FROM THE NUMBERS ON THE SLIDES TEENS ARE VERY ONLINE, ENGAGED WITH MOBILE

APS AND SOCIAL MEDIA PLATFORMS, THEY'RE DOWNLOADING APS AT LEAST ONCE A MONTH, USING SOCIAL MEDIA MULTIPLE TIMES DAY AND OFTEN OWNING THEIR OWN SMART PHONE DEVICES, THIS IS GENERATIONS BEING REFERRED TO AS DIGITAL NATIVES BECAUSE THEY GROUP WITH THIS TECHNOLOGY AND USE IT SO OFTEN IN THEIR DAY-TO-DAY LIFE AND CREATES THE MISSION THAT TEENS ARE FULLY AWARE OF THE RISKS THAT MIGHT BE INVOLVED WITH ONLINE ENGAGEMENT AND ABLE TO PROTECT THEMSELVES FROM POTENTIAL WRENCHES, IN FACT, YOU CAN SEE 72% OF TEENS DO BELIEVE TECH COMPANIES MANIPULATE USERS, HOWEVER THE PRINTING THEY'RE ABLE TO HANDLE THEMSELVES ON LINE IS THEY'RE EXCLUDED IMPORTANT POLICY DISCUSSION ABOUT PRIVACY.

RIGHT NOW, THE FOCUS REMAINS ON THE CHILDREN ONLINE PRIVACY PROTECTION ACT APPLIES TO CHILDREN UNDER 13 AND PROTECTING YOUNG CHILDREN ONLINE, THERE'S NO RECOGNITION TEENAGERS HAVE THEIR OWN NEEDS ONLINE.

WE HAVE DRIVING IN THE UNITED STATES YOU HAVE TO BE 16 TO GET YOUR DRIVER'S LICENSE OR VOTE YOU HAVE TO BE 18, BUT THERE'S NOTHING LIKE THAT ONLINE.

AND THIS IS REFLECTED BY THE PROPOSED LEGISLATION THAT YOU CAN SEE ON SCREEN THAT RELY GATES TEENAGERS TO THE SAME RESTRICTIONS IMPOSED ON YOUNGER CHILDREN, AND IT'S UNREAL ATLANTIC TO THINK THAT TEENS WILL GET PARENTAL CONSENT LIKE REQUIRING FOR CHILDREN UNDER 13,

THE SAME MEASURES WILL NOT BE EFFECTIVE FOR TEENAGERS BECAUSE THEY BEHAVE AND ENGAGE ONLINE DIFFERENTLY THAN YOUNGER CHILDREN STUDY SHOW HAS GREATER PRIVACY RISKS, TEEN DIRECTED APS KANYE WEST HIGH LEVEL OF PERMISSIONS 11 MEDIAN PERCS WERE REQUESTED AND SIX MEDIAN PERMISSIONS WERE REQUESTED.
AND THEY ALSO HAD A HIGH LEVEL OF TRACKERS.
THEY'RE A MEDIAN OF TEN TRACKERS INTEGRATED IN TEEN DIRECTED APS.
MORE DIRECT COMPARISON YOU CAN SEE THAT OUR KEY FINDINGS SHOWED THAT A MAJORITY OF TEEN DIRECTED APS WERE SUPPORTED BY ADS, 82% VERSUS LESS THAN HALF OF OUR GENERAL APS WE LOOKED AT.
BEFORE I GET INTO MORE DETAIL ABOUT OUR FINDINGS, I'LL TALK ABOUT METHODOLOGY, SO AS THE TITLE INDICATES, WE PULLED SET UP AS FROM THE GOOGLE PLAY STORE BECAUSE GOOGLE HAS ENTIRETY CONTROL SO IT'S MORE DIFFICULT TO ANALYZE THEM, WE LIMITED OUR STUDY TO THREE APS, SO WE HAVE TWO DATA § STUDY AS YOU CAN SEE ON THE SCREEN, GENERAL DATA SET WHICH WE USED AS A POINT OF COMPARISON TO BE BE REPRESENTATIVE OF THE AP STORE BY SCRAPING THE TOP 200 APS FROM THE TOP GENRE AND GOT THE SUGGESTED APS FROM THOSE TOP 200 APS IN EACH GENRE WHICH LED US TO GET A DATA SET OF ALMOST 54,000 APS.
OUT OF THOSE WE NARROWED IT DOWN TO GET OUR TEEN DIRECTED DATA IT IS.
WE DID THIS USING COUPLE

METHODS.
FIRST PULLED THE AP THAT IS HAD TWEEN MILLION OR MORE INSTALLS AND APPLIED A MULTI-FACTOR FRAMEWORK WE CREATED TO FIGURE OUT WHICH APS WERE LIKELY TEEN DIRECTED OUT OF THOSE AND TO FIGURE OUT THAT MULTI-FACTOR FRAMEWORK WE ADOPTED THE FTC FACTORS FOR DETERMINING CHILD DIRECTED SERVICES TO TEENAGERS LOOKING AT SUBJECT MATTERS AND CELEBRITY MIGHT APPEAL TO TEENAGERS THEN LOOKED AT INDUSTRY STANDARDS OUT THERE LIKE THE MPAA RATINGS FOR MOVIES AND THE ESR RATINGS FOR VIDEO GAMES TO SEE WHAT THEY RATE THE AS APPROPRIATE CONTENT FOR TEENAGERS AND OUR OWN GENERAL KNOWLEDGE OF WHAT TEENS, APS LIKE TIKTOK IS INCLUDED OBVIOUSLY AND FINALLY WE FINALLY GOT A DATA SET OF A LITTLE BIT OVER 1100 APS THAT WERE LIKELY TEEN DIRECTED.
WHICH OUR TEEN THEN USED STATIC ANALYSIS ON TO GENERATE FINDINGS.
FIRST I WANT TO TALK ABOUT THE MONTE SENSATION METHODS, IN OUR STUDY, FIRST BEING ADVERTISING, FOR BACKGROUND TWO TYPES OF ADVERTISING, CONTEXT RELAY IT SIMPLY LOOKS AT THE CONTENT THAT A TEEN USER IS LOOKING AT TO FURTHER INTEREST AND ADD A BASE ON THAT CONTEXT, THE SECOND ADVERTISING IS A LITTLE BIT MORE INVASIVE CALL INTRA SPACED ADVERTISING CALLED TARGETED OR BEHAVIORAL ADVERTISING BECAUSE IT RELYS ON DATA COLLECTED ABOUT THE TEEN USER'S BEHAVIOR TO

SERVE THEM AN AD AS YOU CAN SEE
IT SHOWS HOW IT'S COLLECTED AND
HANDED OVER TO VARIOUS THIRD
PARTIES AND RE PACKAGED AND
ADVERTISING SEND BACK TO TEEN
USERS, TARGET ADS MAY NOT SOUND
LIKE BAD THING, TEENS ARE
ALREADY EXPOSED TO 30% MORE
ADVERTISING ACROSS THE BOARD
THAN GENERAL AUDIENCES, IN
ADDITION, WHAT OFTEN HAPPENS IS
PERIPHERALS ARE BUILT AROUND
TEEN USERS USING THE DATA WHICH
REVEALS A FULL PICTURE OF THEIR
LIFE INTEREST .
SECOND TYPE WE LOOKED AT'S THESE
ARE WAYS APS GENERATE REVENUE BY
SPENDING THINGS ON POWER APS
UPGRADES OR EXTRA CONTENT IN AN
AP.
STUDY FOUND IN ADDITION TO
SEEING MORE ADS THEY'RE GETTING
BOMBARDED IN MUCH HIGHER VOLUME.
AS YOU CAN SEE THERE WAS ABOUT
FOUR TIMES AS MANY GENERAL
AUDIENCE APS WITH IN AP PURCHASE
WITH THOSE WITHOUT BUT IN THE
TEEN DATA IT IS THAT SKY
ROCKETED TO ABOUT 13 TIMES AS
MANY THAT OFFERED IN AP
PURCHASES THIS BECOMES
ESPECIALLY PROBLEMATIC BECAUSE
THEY USE DARK PATTERNS LET'S
THEM USE MORE TIME AND MONEY
THAN THEY WOULDN'T ORDINARILY, R DISCHOSE WHAT THEY'RE
DOING.
IT'S ON USERS TO READ, FOR EXAMPLE, THAT
INFORMATION.
IF IT'S IN A USABLE FORMAT.
WE KNOW PRIVACY POLICIES PEOPLE ARE NOT REALLY
READING.
I THINK PEOPLE SHOULD EDUCATE THEMSELVES.
HOWEVER THIS INFORMATION SHOULD BE AVAILABLE.
I THINK THIS IS, WE HAVE A GAP, HUGE GAP.

WE WOULD LIKE MANUFACTURES TO TELL CON SYMEERS IN A UNDERSTANDABLE LANGUAGE WHAT THEY'RE DOING AND HOWER THAT PROTECTING THEM.
BASICALLY THE PRACTICE THAT'S ARE RELEVANT TO CONSUMER AND CONSUMER DATA. IF THE INFORMATION IS AVAILABLE YES.
THEY NEED TO READ THE INFORMATION.
CONSUMERS NEED TO EDUCATE THEMSELVES.
IF THEY SEE SOMETHING THAT IS QUESTIONABLE TO THEM THEY NEED TO FOR EXAMPLE CONTACT THE MAN AOU FAM TOURER OR CONTRACT PRIVACY EXPERTS F THEY KNOW THEM OR RAISE THAT CONCERN.
SO OTHERS MORE EXPERT IN THE ISSUE CAN HELP THEM OR AT LEAST HELP CONSUMERS HELP THEMSELVES.
>> IN YOUR RESEARCH DID YOU FIND INSTANCES WHERE RISK PERCEPTION WAS NOT ALIGNED WITH THE CONSUMER WILLING TO PURCHASE THE PRODUCT.
>> GREAT QUESTION.
MOST CASES THESE TWO WERE ALIGNED.
WHICH BASICALLY THINK MAKES SENSE.
THERE ARE A FEW EXCEPTIONS.
FOR EXAMPLE CONSUMERS UNDERSTOOD THE RISK BUT THAT RISK WAS NOT ENOUGH FOR THEM TO CHANGE THEIR DESIRE TO PURCHASE THE DEVICE.
FOR EXAMPLE MULTI FACTOR AUTHENTICATION.
PEOPLE KNOW THIS WILL DECREASE THE RISK.
THEY PERCEIVE LOWER RISK, MULTI FACTOR IDENTIFICATION.
THEN THEY TOLD US THIS INFORMATION IS NOT GOING TO BASICALLY HELP THEM PURCHASE THE DEVICE.
IN SOME CASES PURCHASES WOULDN'T PURCHASE BECAUSE OF MULTI FACTOR AUTHENTICATION AND USEIBILITY CHALLENGES.
ANOTHER CHALLENGE WAS SECURITY UPDATE.
PEOPLE KNEW AUTOMATIC UPDATE IS BETTER THAN NO UPDATE OR BETTER THAN MANUAL UPDATES IN TERMS OF RISKS.
HOWEVER THEY SAID THEY WOULD LOVE TO HAVE CONTROL.
THEY PREFER MANUAL UPDATES OR AUTOMATIC UPDATES.
IT SHOWS RISK IS NOT ENOUGH.
THIS T. SHOULD -- THE PRACTICE SHOULD BE DESIGNED AND USABLE WAY SO THAT NOT ONLY IT CONVEYS A RISK, DECREASES THE RISK, THEY'RE ALSO USABLE.
PEOPLE ARE INTERESTED IN USING THEM AND GOING TO

PURCHASE THE DEVICE BECAUSE OF THE FEATURES NOT
GOING TO TURN AWAY BECAUSE OF USE ABILITY ISSUES.
>> IT WAS INTERESTING YOUR PAPER REPORTED ON SELF
REPORTING PURCHASE BEHAVIOR OF CONSUMERS THERE.
IS DEBATE ON WHAT PEOPLE SAY AND WHAT THEY ACTUALLY
DO RELATEING TO PRIVATE SEE.
DO YOU HAVE THOUGHTS OR EXPECTATIONS HOW YOUR IOT
LABEL I COME PACT REAL PURCHASEING BEHAVIOR
>> GREAT QUESTION.
I THINK THE MAIN REASON WE DID THIS STUDY, THIS LINE
OF STUDY ON SELF REPORTING FASHION IS THAT WE DO NOT
HAVE THE LABELS.
WE CAN NOT HAVE THE LABELS IN THE REAL PURCHASE
BEHAVIOR.
DEVICES DON'T HAVE LABELS BASICALLY.
WE CAN'T REALLY TEST THAT.
IF YOU LOOK AT OTHER LITERATURE, FOOD LITERATURE WE
KNOW THAT CONSUMERS WHO ARE MORE INTERESTED IN
HAVING BETTER HEALTH FOR EXAMPLE, THOSE ARE THE ONES
THAT LOOK INTO NUTRITION LABELS OR THOSE WHO HAVE
MORE KNOWLEDGE LOOK INTO NUTRITION LABELS.
THOSE ARE DIFFERENT FACTORS HOW INTERESTED YOU ARE
LOOKING FOR THE INFORMATION.
HOW THE INFORMATION IMPACTS YOUR PREFERENCES AND
DESIRE TO PURCHASE, FOR EXAMPLE THE DEVICE.
SUCH AS INTEREST.
SUCH AS NOTHING.
KNOWLEDGE.WE DON'T KNOW HOW OUR LABEL WILL IMPACT PURCHASE
BEHAVIOR.
BASED ON WHAT WE HEARD FROM CONSUMERS ON STUDIES
THAT WE CONDUCTED WE KNOW THE LABEL IS
UNDERSTANDABLE.
WE DON'T KNOW IF THAT WOULD CHANGE THEIR WILLINGNESS
TO PURCHASE IF WE PRESENTED THE ACTUAL PURCHASE
BEHAVIOR.
>> I'M GLAD YOU GOT THE KORPBGS PROBLEMS FIXED.
WELCOME BACK.
>> THANK YOU.
>> I WANTED TO GO BACK TO THE QUESTION BEFORE YOU
TKR-PD OFF.
WHETHER THE IOT WATCH TOOL IS STILL IN DEVELOPMENT
AND WHETHER THERE ARE PERHAPS TO MAKE IT AVAILABLE
TO RESEARCHERS OR OTHERS.
>> GREAT QUESTION.

THIS IS FOR THE SMART THINGS PLATFORM.
WE WOULD LIKE TO MAKE THE TOOL AVAILABLE DOWN THELY AND HAVE IT FOR OPEN HAB AS WELL.
FOLLOWING COMPLETE PRIVATE SEE OF THE TOOL.
AT PRESENT WE HAVE A DEMO AVAILABLE AT I TO.WATCHSPOT.COM.
YOU CAN PUT IN THE SOURCE CODE -- SO THAT INSTRUMENTAL SOURCE CODE WON'T BE USED BY ANYTHING.
THE PORTION OF IOT ANALYZER IS NOT PUBLICLY AVAILABLE YET.
THE DEMO IS AVAILABLE TO SEE WHAT IT WOULD DO TO THEIR OWN CODE.
>> THAT'S GREAT.
I UNDERSTAND, CORRECT ME IF I'M WRONG.
THE WAY IOT WATCH WORKS IS IT SAYS DATA TO AN ANALYSIS.
ARE THERE MEASURES TO PROTECT THE DAT AMOUNT
>> YES.
IT USES TLS TO SECURE.
IOT WATCH DOESN'T COLLECT A IDENTIFIABLE INFORMATION.
ALSO OUR TOOLS DON'T FINGERPRINT OR EXPOSE USER ACTIVITY WHATSOEVER.
BECAUSE IOT WATCH DOESN'T COLLECT INFORMATION AND STORE IT.
IT SENDS THE INFORMATION, ANALYZES IT, AND SENDS IT BACK.
WE ALSO INCLUDE A TUTORIAL TO EXPLAIN WHAT WE DO WITH THE INFORMATION WE COLLECT.
THAT CAN BE FOUND IN THE PAPER AS WELL.
>> IF A DEVELOPER USED ENCRYPTION WOULD THAT ALLOW THEM TO EVADE IOT WATCH'S ANALYSIS
>> SO THE WAY IOT WATCH WORKS NOW.
IT DOESN'T ACCOUNT FOR ENCRYPTION.
IF A APP WAS FOUND TO ENCRYPTING IT'S STRINGS THERE WOULD BE WAYS AROUND IT.
IN THE CASE OF A APP INFLUENCES ENCRYPTION THE APP WOULD HAVE TO IMPLEMENT THE ENCRYPTION BEFORE SENDING THE FUNCTION IT COULD BE MODIFIED TO EXTRACT BEFORE.
EXPOSING THE IOT STREAM.
HOWEVER WE FOUND THAT IS ACTUALLY A MOOT POINT FROM WHAT WE HAVE SEEN SO FAR.
OUT OF THE SMART THINGS APP WE LOOKED AT NONE ENCRYPTED FURTHER THAN THE TLS ENCRYPTION LAYER.

IF WE ENCOUNTERED A APP ENCRYPTING DATA THAT WOULD OF FLAG IT DID SUSPICIOUS TO US.
>> YOU KNOW I'M SORT OF INTERESTED IN THE THOUGHTS FROM EVERYONE ON THE PANEL ABOUT FUTURE AREAS OF RESEARCH REGARDING IOT THAT YOU THINK WOULD BE PARTICULARLY USEFUL.

>> I DEFINITELY THINK THAT ONE OF THE BIGGEST AREAS OF RESEARCH OR DEVELOPMENT IN THE IOT SPACE NEEDS TO BE REGULATION FOR DESCRIBING THE PRIVACY IMPACTS OF IOT DEVICES TO CONSUMERS.
I THINK THAT IF SOMETHING LIKE THAT WAS IN PLACE WE WOULDN'T BE ABLE TO, IOT WATCH WOULDN'T BE NECESSARY.
THE APP WOULD EXPOSE WHAT THEY DO WITH PRIVATE INFORMATION THEMSELVES.
IN TERMS OF LIKE FUTURE RESEARCH WE NEED TO JUST BE LOOKING AT BETTER WAYS OF ANALYSIS, MAYBE MORE DYNAMIC ANALYSIS AND STATIC ANALYSIS TO ANALYZE HOW APPS ARE RUNING AND WHAT THEY DO WITH THE INFORMATION THAT USERS PUT IN AND THE INFORMATION THAT THE APPS THEMSELVES ARE DEALING WITH IN TERMS OF LIKE WHETHER A DOOR IS OPEN OR THINGS LIKE THAT.
>> OKAY.
>> SO, I THINK WHAT I FEEL IS MISSING HERE IS REALLY THE REALISTIC PUR SETTINGS AND REALLY UNDERSTANDING THE CONSUMERS UNDERSTAND PRIVACY AND SAFETY AT THE TIME OF PURCHASE AND THE POINT OF SALE.
THINK IN OTHER COUNTRIES LINE FINLAND AND SINGAPORE WE HAVE THE LABELS.
WE DON'T HAVE IT IN THE U.S. FOR SURE.
I THINK IF MANUFACTURES ARE FOR EXAMPLE GOING TO ADOPT A LABEL, MAYBE TO JUST BE IN A PILOT STUDY TO A DIDN'T A HAEUBL.
WE CAN STUDY THEM AND SEE WHETHER CONSUMERS UNDERSTAND THE INFORMATION.
WHETHER THEY UNDERSTAND THE RISK AND THINGS LIKE THAT.
I THINK THIS IS IMPORTANT HERE.
THIS CAN PUSH THIS OF THE FORWARD A LOT.
WE CAN NOT JUST CONTINUE WORKING ON SELF REPORTED RESPONSES.
WE WANT TO UNDERSTAND THE REALISTIC BEHAVIOR.
THINK THE NEW WHITE HOUSE EXECUTED ORDER WORK

TOGETHER TO BASICALLY CONDUCT A PILOT AND LOOK NO
THE EFFORTS INTO LABELING THE SMART DEVICES.
I THINK THIS IS NOW GAINING SOME INTEREST IN THE
U.S. AS WELL.
I AM ACTUALLY OPTIMISTIC ABOUT THIS.
THIS IS BASICALLY THE U.S. IS LOOKING INTO THIS
EFFORT.
MAYBE IN THE NEAR FUTURE WE WILL HAVE THESE LABELS
FOR DEVICES AND A WHOLE NEW SET OF RESEARCH STUDIES
WILL BASICALLY BE CONDUCTED AFTER WE HAVE THOSE
LABELS.
>> YES, SO FOR THE CONTEXT OF VOICE INTERFACES ONE
OF THE INTERESTING RESEARCH QUESTION IS GOING TO BE
HOW DO WE DESIGN EFFECTIVE INDICATEERS OR
INTERVENTIONS FOR VOICE INTERFACES.
WHEN USERS INTERACT WITH VOICE INTERFACES THEY THING
WHO EVER THE VENDOR IS THAT'S THE COMPANY DOING THE
WORK.
WHEN YOU OPEN THE MAT FORM FOR A THIRD PARTY IT'S
MORE TRICKY.
I THINK DESIGNING EFFECTIVE INDICATEERS OR VOICE EN
TER SREPGSS I THINK THAT IS CHALLENGEING AND HADS
INTERESTING BECAUSE WE NEED THAT.
WE KNOW USERS DON'T CHECK ALL OF THE INFORMATION BY
THEMSELVES.
WE FEED TO CHECK THROUGH INTER ACTIONS AND PRAAT
FORMS.
I THINK THAT'S A OPEN RESEARCH PROBLEM WE WILL SEE
IN THE FUTURE.
>> WHAT BUT, JEFFREY, YOUR THOUGHTS.
>> ONE OF THE THINGS I THINK WE HAVE FOUND OVER
TESTING THIS FAR IS THAT DEVELOPERS DON'T BELIEVE
THEY'RE VIOLATEING POLICY.
THEY'RE DEVELOPING CODE IN THE BEDROOM OR THAT.
I SEE OUR FIELD BEING ABLE TO TEST SOURCE CODE
BEFORE IT GOES TO THE PLATFORM.
SO SOME SORT OF TOOL TO TEST.
ALSO DYNAMIC PERMISSION MODELS.
BECAUSE IT'S VOICE INTER ACTION IT'S DIFFICULT TO
ASK PERMISSION.
HOW CAN YOU DESIGN A PERMISSION MODEL THAT IS
ACCURATE AND INFORM THE CONSUMER.
DO YOU GIVE PERMISSION TO THIS SKILL FOR THIS DATA
AT THIS PARTICULAR POINT.

THAT SORT OF QUESTION.
THAT WILL PROBABLY BE AN OPEN QUESTION FOR A WHILE BECAUSE OF THE PLATFORM ITSELF.
>> GREAT.
SO WE ARE ABOUT THE END OF OUR TIME.
I WANT TO ENCOURAGE EVERYONE TO GO TO THE PRIVACY PAGE OF FTC GOV TO READ PRESENTERS FULL RESEARCH PAPERS THEY'RE WELL WORTH YOUR TIME.
WE ARE GOING TO TAKE A SHORT BREAK.
PLEASE STICK AROUND FOR A PANEL ON PRIVACY, CHILDREN AND TEENS.
I WANT TO THANK OUR PANELISTS FOR THEIR WORK, RESEARCH, AND SHAREING WITH US TODAY.
THANK YOU EVERYONE AT HOME FOR JOINING US.
§
(BREAK)
§
>> OPERATED IN A REACTIVE MANNER WITH SIGNIFICANT THREAT TO USERS.
NEXT SLIDE, PLEASE.
THE PANDEMIC HAS CHANGEED DAILY LIFE FROM ACROSS THE GLOBE.
FIRST OF ALL WIDESPREAD LOCK DOWN.
TRAVEL RESTRICTION, WORK FROM HOME ARRANGEMENT HAVE INCREASED USER ALLIANCE ON A LOST SERVICES.
SECT THE DATA FROM DIFFERENT SOURCES HAVE CAUSED PANIC AMONG PEOPLE.
THIRD PEOPLE DESIRE TO HELP EACH OTHER WHO WERE ESPECIALLY WHO WERE AFFECTED DURING THE GLOBAL DISASTER.
UNFORTUNATELY THIS INCREASED USAGE OF THE INTERNET HAS LEFT -- PHISHING AND SCAM MORE THAN EVER.
NEXT SLIDE, PLEASE.
SO LET'S SEE SOME OF THE EXAMPLES OF THESE.
THE PHISHING WE'RE TALKING ABOUT AND PEOPLE ARE ENCOUNTERING.
PEOPLE WERE SENT A HUGE VARIETY OF E-MAILS THAT IMPERSONATE AUTHORITIES SUCH AS CD TKR-RBGS AND ASKING THEM TO DONATE TO BOGUS CAUSES.
NEXT SLIDE, PLEASE.
FOR EXAMPLE THIS ONE IS AN E-MAIL THAT SAYS TO BE SENT FROM CDC AND ASKING PEOPLE TO DONATE BIT COIN TO FUND COVID-19 RESEARCH.
THE OTHER EXAMPLE LOOKS LIKE MICROSOFT OUTLOCK

INTERFACE.
IT ASKS FOR USER NAME AND PASSWORD TO SHOW INFORMATION ABOUT NEW CASES OF INFECTION AROUND YOUR CITY.
NEXT IS THE EXAMPLE THAT WE SEE DIFFERENT IN SPAM CAMPAIGNS USING FACE MASKS OR GLOVES.
THESE ARE JUST A FEW EXAM AND THIS ARE MUCH MORE OUT THERE.
NEXT SLIDE, PLEASE.
SO, TO FIND THESE TRENDS AND TO UNDERSTAND HOW THE PHISHING TREND CHANGES WE COLLECT A DIFFERENT VARIETY OF DATA SETS.
WE COLLECTED NEWS ARTICLE AND GOVERNMENT ANNOUNCEMENT ABOUT PHISHING AND SCAM RELATEED TO PANDEMIC.
WE ALSO COLLECTED CORONA RELATEED DISCUSSIONS FROM TWO UNDERGROUND FIRMS TO UNDERSTAND HOW CYBER CRIMINAL ACTIVITY CHANGED DURING THE PANDEMIC.
THEN WE GATHER -- ISSUE CERTIFICATES AND REPORTED PHISHING WEB SITES TO SEE HOW THE PANDEMIC AFFECTED INFRASTRUCTURE.
THEN TO UNDERSTAND WHAT KIND OF CONTENT HAS BEEN USED WE PULLED THE SOURCE CODE OF THE MALICIOUS WEB SITES.
WE COLLABORATEED WITH THE ORGANIZATION AND USED SPECIALIZED NETWORK MONITOR TO ANALYZE SRUBG TIMS TRAFFICED TO PHISHING WEB SITES AND VOLUME OF PHISHING.
UNFORTUNATELY DUE TO TIME LIMITATION I'M NOT GOING TO TALK ABOUT THE FIRST TWO DATA SET.
THE FIRST IS FOUR MONTHS OF 2020.
NEXT SLIDE, PLEASE.
IN THE FIRST STAGE OF THE STUDY WE OBSERVEED THE NUMBER OF PAOUS RELATEED TO COVID-19 AND HAD RAPID GROWTH.
WE FURTHER INVESTIGATED THE MAT ARE AND LOCKED AT THE REGISTRATION PATTERNS.
WE COLLECTED THE SOURCES FROM ZIT SOURCES.
FUNDING CORONA DOMAIN MAIM.
TO UNDER THE ACTIVITY ACTUALLY IF THEY'RE USED OR REGISTERED POOR OTHER PURPOSES.
WE LOCKED AT THE CERTIFICATES.
WE CALL IT 144M AND OTHER HAVE THE INDICATES USING GOOGLE ROCKETEER, IF YOU LIKE.

THE FIGURE ON THE TOP SHOWS THE NEWLY REGISTERED CORONA DUMMY FAMES STARTED TO INCREASE FROM MARCH.
-- W.H.O. DECLARED THE EMERGENCY AND THE TIME THAT W.H.O. DECLARED THE OUT BREAK OF COVID-19 PANDEMIC.
AS THE NUMBER OF CORRELATED NAMES INCREASE IT'S HARDER TO DISTINGUISH GOOD WEB SITES AND MALICIOUS ONES.
-- INCREASED FROM BE IF AND MARCH.
NEXT PLEASE.
OKAY SO FAR WE HAVE SEEN THE PATTERN AND CERTIFICATE PATTERN.
FOR THE NEXT STEP WE LOOK AT THE WEBSITE PHISHING WEBSITE BEING REPORTED.
THE NUMBER REPORTED TO TWO MAJOR HOUSES OF URLs, APWG AND OPEN DIDN'T INCREASE SIGNIFICANTLY DURING COVID-19.
HOWEVER THEY FAILED TO ACCURATE REFLECT THE DAMAGE CAUSED BY COVID.
HIGH IMPACT WEB SITES RECEIVE MORE TRAFFIC BECAUSE OF SPAMING ACTIVITY OR EVADING DEFENSES.
SO TO DEEPEN OUR PHISHING TRENDS WE LOOKED NO A MONITORING APPROACH.
I WILL TALK TO THIS IN HIGH LEVEL.
PHISHING WEB SITES OFTEN ATTRACT CODE OR IMAGES THAT ARE HOSTILE ON EXTERNAL SERVERS.
FOR EXAMPLE PHISHING WEBSITE IMPERSONATING MICROSOFT.
WE SEE THREE OF THEM GO TO THE SERVER OF THE ORGANIZATION.
IF WE'RE ABLE TO TRACK THESE WEB EVENTS WE CAN TRACK TO A PHISHING WEBSITE.
HOWEVER TO HAVE THE DATA ONE IS THE ORGANIZATION THAT IS ACTUALLYLY TARGETED BY ATTACKERS.
WE COLLABORATED WITH SUCH ORGANIZATION AND ANALYZED TWO ADDITIONAL DATA SET.
TRAFFIC TO PHISHING WEB SITES BY TARGETED VICTIMS AND PHISHING REPORTED TO THE ORGANIZATION.
NEXT SLIDE PLEASE.
AS SHOWN IN THE FIGURE THE NETWORK MONITOR RECORDED A SUDDEN IN CREASE OF VICTIMS IN MARCH ELEVATEING IN APRIL.
IN MARCH AND APRIL WE CAN SEE 2.1 AND 1.6 TIMES MORE VICTIMS THEN JANUARY.
JANUARY IS THE TIME THAT THE ORGANIZATION USUALLY

SEES ELEVATED ACTIVITY BECAUSE OF THE HOLIDAY SHOPPING SEASON.
ALSO THE NUMBER OF E-MAILS REPORTED TO THE ORGANIZATION VALIDATED THE INCREASE ACTIVITY.
NEXT SLIDE, PLEASE.
SO, WE SEE THAT THE NUMBER OF PHISHING WEB SITES REPORTED DID NOT INCREASE SIGNIFICANTLY.
ON THE OTHER HAND WE HAVE THE NUMBER OF VICTIMS.
THE QUESTION ARISEED WHAT IS THE CONTACT THAT ATTRACTS VICTIMS.
WE CROWD THEM AND GROUP NO FOUR MAIN CATEGORIES.
FIRST IS THE VICTIM WOULD THINK THEY'RE MAKING A SMALL DONATION.
HOWEVER INSTEAD THE ATTACKER STEALS THEIR INFORMATION.
THE OTHER CATEGORY IS PP SALE.
PERSONAL PROTECTIVE EQUIPMENT WAS IN HIGH DEMAND AND SHORT SUPPLY.
ATTACKERS EXPLOITED THIS AND CREATED FAKE WEB SITES.
NEXT SLIDE, PLEASE.
ATTACKERS ARE ALSO EXPLOITING EVENTS RELATEED TO CORONA.
TO UNDERSTAND THE FINANCIAL HARDSHIP THE U.S. GOVERNMENT OFFERS STIMULUS PAYMENT.
HOWEVER DIFFERENT GROUP OF PEOPLE RECEIVE THE PAYMENT IN DIFFERENT TIME.
WHEN THOSE WHO RECEIVE THEIR CHECKS SHARED ABOUT IT ON SOCIAL MEDIA OTHERS STARTED TO WORRY IF AND WHEN THEY WOULD RECEIVE THEIR PAYMENT.
SO PHISHING DISGUYSED THEMSELVES AND STOLE THEIR INFORMATION.
THE FINAL CATEGORY IS A SHOPPING WEBSITE.
FRAUDULENT SHOPPING WEBSITE TROY TO KEEP UP WITH THE LOOK AND FOAL OF LEGITIMATE WOULD BE SITE AS MORE AND MORE LEGITIMATE ORGANIZATION INCLUDE COVID 19 RELATEED INFORMATION IN THE WEBSITE SUP AS STA AT THIS TIMEICS AND NEW POLICIES.
PROFESSIONAL WEB SITES ALSO INCLUDE SUCH INFORMATION.
MECHANICS SHOWED, PLEASE.
I HAD WRAP THIS PRESENTATION WITH OUR KEY TAKEAWAYS EVEN IN OUR DATA SET THE NUMBER OF PHISHING ATTACK LEVERAGEING THE PANDEMIC SEEMS TO BE -- THIS ARE STILL RECORD BREAKING NUMBER OF VICTIMS.

WE BELIEVE THIS IS BECAUSE THE ATTACKERS -BGS
LIGHTED PANDEMIC, PEOPLES PANDEMIC RELATEED WANTS
AND MODES WITH HIGH QUALITY WEB SITES.
ALSO WE OBSERVE THAT THE NUMBER OF NEWS RELATEED TO
THE PANDEMIC INCREASED IN MARCH.
HOWEVER THERE ARE STILL MANY VICTIMS.
THIS IMPLIES THAT, HIGH PHISHING SYSTEMS IS NOT
ENOUGH TO PRO T-BGT USERS.
NEXT PLEASE.
WE COLLECTED 467,000 DOMAIN NAMES REHATED TO COVID.
17,000 CERTIFICATE ISSUE RELATEED TO DOMINANCE, LESS DOMAINS.
LESS THAN ONE PERCENT -- LESS THAN THOUSAND ARE
BENIGN.
THE OTHER HAPPENED WE HAVE THE FTC REPORT SHOWING
PEOPLE LOSEING FOUR MILLION DOLLARS TO COVID-19
RELATEED FRAUD FROM JANUARY TO MAY.
THIS I AM PLOYS THAT FISHING IS ONE TYPE OF CORONA
RELATEED ATTACK.
THIS ARE OTHER TYPES THAT OTHERS SHOWING CYBER
CRIMINALS ARE EXPLOITING THE SYSTEM LACK OF DEFENSE
AGAINST OTHERS.
NEXT SLIDE, PLEASE.
THANK YOU.
>> THANK YOU, VERY MUCH FOR YOUR INTERESTING
PRESENTATION.
NEXT WE HAVE CHRISTINE GEENG.
CHRIS TONE IS A PH.D. CANDIDATE AT THE UNIVERSITY OF
WASHINGTON.
HERE TO TALK ABOUT HER PAPER.
>> NEXT SLIDE.
JUST TO GIVE AN OVER VIEW OF THE PROJECT I WILL
PRESENT WE CONDUCTED A MIX METHOD SURVEY ON SOCIAL
MEDIA USERS ATTITUDE TOWARDS FALSE INFORMATION
LABELS.
THIS WAS CONDUCTED IN MARCH 2020 OVER THE BEGINNING
OF THE PANDEMIC.
NEXT SLIDE.
SO, IT'S PROBABLY NOT NEWS TO ANYONE HERE THAT
CORONAVIRUS MISINFORMATION IS A MAJOR PROBLEM ON
HORRIBLE KPHAOED YA WHEN THE PANDEMIC FIRST POPED UP
ON FACEBOOK ACCORDING TO THIS GRAPH IN A COUPLE OF
WEEKS AFTER THE FIRST POSTING IT HAD MILLION MORE
INTERACTIONS THEN OTHER POPULAR VIDEOS UP LOADED TO
FACEBOOK AROUND A SIMILAR TIME.

NEXT SLIDE.
SO, GIVEN THE SEVERITY OF THE ISSUE PLATFORMS HAVE TAKEN STEPS TO RAMP UP MISINFORMATION ACTION.
FOR EXAMPLE INCREASING FACT CHECKING AND LABELING POSTS.
SO IN THIS EXAMPLE.
THIS IS A SCREEN SHOT OF FACE BOOK'S FALSE INFORMATION LABEL THAT THEY OVER LAY CERTAIN POSTS.
NEXT SLIDE.
PLATFORMS HAVE ALREADY STARTED PARTNERING WITH HEALTH ORGANIZATIONS LIKE THE CDC AND THE WHO.
IF YOU GO TO INSTAGRAM AND SEARCH TO ANYTHING RELATE TO THE CORONAVIRUS YOU WILL SEE A GENERIC BANNER THAT SAYS USERS CAN GO TO THE CDC FOR TRUSTED HEALTH INFORMATION.
NEXT SLIDE.
OF COURSE WITH AWFUL THESE NEW LABELS AND INTERVENTIONS THAT PLATFORMS HAVE THIS RAISES THE QUESTION OF HOW EFFECTIVE THEY ARE IN COMBATING THE INFORMATION.
SO PRIOR RESEARCH DONE ON FACE BOOK HAS SHOWN THAT HAVING A RELATEED STORY FACT CHECKER LABEL AS IN THIS IMAGE CAN SIGNIFICANTLY CORRECT MISINFORMATION.
THOSE ARE THE LABELS ON FACEBOOK IN 2017.
THEY HAVE CHANGED THE KINDS OF INTERVENTIONS THEY HAVE USED SINCE THEN.
NEXT SLIDE.
OF COURSE IT'S NOT ONLY THE PLATFORMS CORRECTING THE INFORMATION ON-LINE.
PRIOR RESEARCH ON TWITTER HAS SHOWN USERS SOMETIMES TAKE STEPS TO CORRECT RUMORS THIS.
DIAGRAM PRESENTS THE MENTAL MODEL OF A TWITTER USER DECIDEING IF THEY WILL CORRECT SOMETHING THEY PREVIOUSLY TWEETED THAT TURNED OUT TO BE FALSE.
WELL, CLEARLY THE CIRCUMSTANCES OF COVID-19 AND COVID-19 MISINFORMATION IS NOVEL.
WE FELT COMPELLED TO STUDY THESE INTERVENTIONED WITHIN THE SPECIFIC CONTEXT.
THAT LEAD TO OUR RESEARCH QUESTIONS.
NUMBER ONE WHAT ARE PEOPLES ATTITUDES TOWARDS SOCIAL MEDIA INTERVENTION FOR MISINFORMATION KHREUDING GENERIC BANNERS.
NEXT SLIDE.
TWO, HOW DO PEOPLE DISCOVER THAT COVID-19

MISINFORMATION IS FALSE.
SPECIFICALLY WHAT WAS THE ROLL OF PLATFORM INTERVENTIONS IN THE DISCOVERY COMPARED TO OTHER METHODS.
NEXT SLIDE.
IN OTHER WORDS TO ANSWER THE QUESTIONS WE CONDUCTED A PAID MIX METHOD SURVEY IN MARCH OF 2020.
DURING THE BEGINNING OF THE PANDEMIC.
WE ALSO FELT COMPELLED TO COLLECT DATA QUICKLY BECAUSE THIS WAS SUCH A NOVEL SCENARIO.
WE RECRUITED THROUGH THE PERSONAL NETWORKS.
OUR STUDY WAS DEEMED EXEMPT.
NEXT SLIDE.
SO, THE FIRST PART OF THE SURVEY CONSISTED OF OPEN-ENDED QUESTIONS AROUND WHAT PARTICIPANTS THOUGHT ABOUT FACEBOOK, TWITTER, INSTAGRAM MISINFORMATION.
WE ASKED THEM TO RATE THOSE ON A 5 POINT SCALE FOR HOW HELPFUL IT WAS.
NEXT SLIDE.
SO TO SHOW WHAT THESE GENERIC WEB BANNERS HAWK LIKE HERE ARE THE BANNERS FROM INSTAGRAM TWITER AND FACEBOOK THAT SAY YOU CAN FIND TRUSTED HEALTH INFORMATION IF YOU GO TO CDC OR A EXTERNAL SITE.
THESE ARE THE POST SPEC TIFF INTERVENTIONS WE ASKED PARTICIPANTS ABOUT. THIS IS FROM TWITTER.
THE HAEUBL OF MANIPULATEED MEDIA AND THE FACEBOOK ONE I SHOWED EAR HERE.
NEXT SLIDE.
IN THE SECOND PART OF THE SURVEY WE ASKED PARTICIPANTS FOR THEIR PRIOR EXPERIENCES OF SEEING COVID-19 MISINFORMATION.
WE ASKED THEM HOW THEY DISCOVERED IT WAS FALSE.
WHAT THEY DID WHEN THEY REALIZED THIS.
NEXT SLIDE.
SO HERE I WILL PRECEPT THE RESULTS FROM THE OPEN-ENDED QUESTION OF HOW PEOPLE FELT ABOUT THE BANNERS.
THE CHART SHOWS THE, HOW WE QUALITATIVELY CODED THE RESULTS.
AS YOU CAN SEE MOST OF THE RESPONDENTS HAD POSITIVE REACTION.
MANY STATED A NEUTRAL RESPONSE.
MANY ALSO STATED THEY FELT THE BANNERS WERE

UNNECESSARY.
THEY WERE ALREADY INFORMED ABOUT CERTAIN HEALTH INFORMATION.
ON THE OTHER END SOME EXPRESSED ANGER AND WORRY THAT THIS COULD BE ABUSEED TO SENSOR INFORMATION IN THEIR WORDS.
NEXT SLIDE.
WE ALSO FOUND THAT PARTICIPANTS RATED POST SPECIFIC INTERVENTIONS MORE HELPFUL THAN GENERIC ONES.
SIGNIFICANT FOR FACE BOOK AND NOT SIGNIFICANT FOR TWITTER.
NEXT SLIDE.
WE ALSO ASKED PARTICIPANTS THE QUESTION OF WHAT DID YOU DO WHEN YOU REALIZED COVID INFORMATION THAT SOMEONE SHARED WAS FALSE.
55% SAID THEY DID NOTHING.
18% SAID THEY CORRECTED THE PERSON PUBLICLY.
17% SAID THEY CORRECTED THE PERSON PRIVATELY.
FOR THE SIMILAR QUESTION, WHAT DID YOU DO WHEN YOU REALIZED COVID-19 INFORMATION YOU BELIEVEED WAS FALSE.
57% SAID THEY NOTHING.
27% SHARED THE CORRECTION.
2% SAID THEY UNSHARED IT IF THEY PREVIOUSLY SHARED THE POST.
NEXT SLIDE.
SO WHAT CAN WE TAKE AWAY FROM THE RESULTS?
FIRST OF ALL SOCIAL MEDIA PLATFORM SHOULD INCREASE SPECIFIC MISINFORMATION LABELING EFFORTS.
THIS IS BECAUSE WE FOUND THAT WE GAINED MOSTLY POSITIVE RESPONSES FROM PARTICIPANTS ABOUT THE INTERVENTIONS AND PARTICIPANTS ALSO FOUND THE SPECIFIC INTERVENTIONS TO BE MORE HELPFUL THAN THE GENERIC BANNERS.
NEXT SLIDE.
WE ALSO WANT TO POINT OUT THAT PARTICIPANTS, NOT JUST SOCIAL MEDIA PLATFORMS CORRECT MISINFORMATION IN VARIOUS WAYS.
NEXT SLIDE.
IN THE OPEN-ENDED RESPONSES PARTICIPANTS DISCUSSED CORRECTING EACH OTHER IN A GROUP CHAT OR ADDING COMMENTS WITH CORRECTIONS TO POSTS OR LIKING EXISTING CORRECTIONS.
SOME PARTICIPANTS MENTIONED REPORTING THE

MISINFORMATION POSTS OR FILTERING UNWANTED CONTENT IN THE FEED.
NEXT SLIDE.
AS WITH ANY STUDY OUR SURVEY CAME WITH CERTAIN LIMITATIONS.
OUR PARTICIPANT POOL WAS A CON SROEPBT SAMPLE NOT REPRESENTATIVE OF THE U.S. POPULATION.
SECOND PLATFORM INTERVENTIONS AND COVID RELATEED NEWS IS RAPIDLY CHANGING.
FINALLY THE INTER SR-PBGSS THAT WE SURVEY PEOPLE ON AND RESPONSES CAME FROM MARCH 20-2, 2020.
IT'S BEEN OVER YEAR SINCE THEN.
A LOT HAS CHANGED ON BOTH PLATFORMS IN TERMS OF THE KIND OF COVID CONSPIRACYS GOING AROUND AND IN GENERAL PEOPLES RELATIONSHIPS WITH COVID AND COVID INFORMATION.
NEXT SLIDE.
WHICH LEADS US TO OUR FUTURE WORK QUESTIONS.
SO FIRST HOW DO YOU USERS RESPOND TO NEW PLATFORM INTERVENTIONS.
NEXT SLIDE.
JUST TO GIVE YOU AN EXAMPLE OCTOBER 2020, TWILLER ROLLED OUT NEW MISINFORMATION LABELS DURING THE U.S. PRESIDENTIAL ELECTION.
SO, IN THIS NEW INTERVENTION THEY LABELED A TWEET AS CONTAINING MISLEADING INFORMATION BUT STATES FOR PUBLIC INFORMATION.
USERS CAN CLICK VIEW AND BE ABLE TO ACCESS THE INFORMATION.
NEXT SLIDE.
FACEBOOK HAS ALSO INTRODUCEED A NEW GENERIC BANNER WHICH BASICALLY TAKES THE USER, THE USERS MORE INFORMATION ON VACCINE INFORMATION.
THEY LABELED ALL WITH VACCINE IN IT WITH THIS GENERIC BANNER.
HOWEVER IT'S STILL UNCLEAR HOW EFFECTIVE HAVING THESE VACCINE INFORMATION LABELS ARE.
AS ONE MOUSE ARTICLE POINTED OUT FACE BOOK KNOWS ADDING LABELS TO TRUMP'S CLAIMS DOES LITTLE TO STOP THE SPREAD.
THE ARTICLE TALKED ABOUT EVEN IF FACEBOOK LABELED TRUMP FALSE CLAIMS MANY STILL SHARED THAT INFORMATION WHICH MEANT THAT COVID MISINFORMATION WAS STILL SPREADING ON THE PALATIFORM THIS.

RAISES A INTERESTING QUESTION OF WHEN IT IS MORE EFFECTIVE TO JUST OUT RIGHT DELETE COVID MISINFORMATION AND CONSPIRACY VERSUS JUST LABELING THEM.
SECOND, THE LAST QUESTION FOR POUT YOU ARE WORK IS HOW CAN PLATFORMS MAKE IT EASIER FOR USERS TO SHARE MISINFORMATION CORRECTIONS.
NEXT SLIDE.
RESEARCH ON THAT QUESTION CAN BUILD ON THE PRIOR WORK OF -- WHO FOUND BEST PRACTICES FOR CORRECTIONS ON SOCIAL MEDIA.
WHICH INCLUDES CORRECTING EARLY, REPEATING CORRECTIONS, INCLUDE A CREDIBLE SOURCE.
NEXT SLIDE.
SO, JUST TO WRAP THINGS UP I HAD REPEAT THE TAKE AWAYS OF THE PRESENTATION.
FIRST POST SPECIFIC INTERVENTIONS ARE MORE EFFECTIVE THAN GENERIC BANNERS.
SECOND WHEN PARTICIPANTS CAME ACROSS FALSE INFORMATION, ABOUT ONE-THIRD MADE A CORRECTION.
FINALLY AS I HAVE SHOWN PLATFORM DESIGNS, COVID-19 MISINFORMATION, AND CULTURAL CONTEXT CHANGE REALLY FAST.
WHICH MEANS THAT THIS KIND OF RESEARCH IS PROBABLY NEEDED OVER A SUSTAINED AMOUNT OF TIME WHICH IS, YOU KNOW OFTEN VERY DIFFICULT.
PARTICULARLY FOR EXTERNAL RESEARCHERS THAT DON'T HAVE THE SAME SORT OF ACCESS TO DATA AS PEOPLE WORKING AT FACEBOOK AND TWITTER NECESSARILY DO.
TO BETTER HOLD THOSE PLATFORMS AVAILABLE NON AFFILIATEED RESEARCHERS SHOULD BE ABLE TO ACCESS THEIR DATA WITH OPEN ACCESS RESEARCH.
>> THANKS.
THIS WORK WAS POSSIBLE THROUGH THE PAUL -- PRIVATE SEW LAB AND CENTER FOR A INFORMED PUBLIC.
THANK YOU FOR LISTENING.
>> THANK YOU BOTH FOR REALLY INTERESTING PRESENTATIONS TODAY.
I WILL JUST OPEN IT UP TO THE Q&A.
STARTING WITH MARZIEH.
WHEN YOU COLLECT THE THE NEWLY REGISTERED DOMAINS COULD YOU TELL WHERE THEY WERE REGISTERED WERE. MOST IN THE U.S.?
>> YES.

IF YOU LOOK AT THE COUNTRY THE DOMAINS WERE
REGISTERED AT.
WE CAN SEE THAT 44% OF THEM WERE REGISTERED IN THE
U.S. FOLLOWED BY GERMANY WITH LESS THAN AROUND 1% OF
THEM.
ALMOST HALF WERE REGISTERED IN THE U.S.
THAT IS ALARMING.
>> FOR SURE.
YOU MENTIONED THAT FOR SOME OF THESE DOMAINS SOME OF
THEM, MOST OF THEM WERE NOT DIRECTLY RELATEED TO
PHISHING RATHER FRAUDULENT SHOPPING WEB SITES ARE.
THERE WAYS FOR CONSUMERS TO KNOW IF THEY'RE ON THESE
TYPE OF SITES?
WHAT TYPE OF ADVICE DO YOU GIVE TO PEOPLE TO MAKE
SURE THEY'RE ON A LEGITIMATE SITE?
>> ACTUALLY THERE IS SOMETHING USERS CAN DO.
LIKE EDUCATION IS REALLY IMPORTANT ABOUT DETECTING
BOTH PHISHING AND SCAMMING WEB SITES.
IT'S NOT LIKE IF WE HAVE A GOOD DIFFERENCE WE DON'T
NEED TO KNOW ABOUT THE WEB SITES.
ONE OF THEM IS MOST TORRENT THING ANYONE CAN DO IS
HAVE BEFORE THEY WRAUPBT TO DO PURCHASE OR ENTER THE
INFORMATION THEY CAN LOCK UP THE PRESENCE OF THE
WEBSITE AND LOOK FOR OTHER PEOPLE EXPERIENCE AND
REVIEWS.
I THINK THIS IS THE MOST BASIC THAT ANYONE SHOULD
DO.
>> AND TURNING TO CHRISTINE, ARE THERE OTHER CLEAR
WAYS SOCIAL MEDIA CAN INCLUDE THE FALSE INFORMATION.
DURING THE PRESENTATION YOU SAY SOME ACKNOWLEDGE THE
LABELS ARE NOT EFFECTIVE.
HAVE YOU THOUGHT OF BETTER WAYS TO PREVENT
MISINFORMATION FROM BEING SPREAD?
>> THAT'S A REALLY GOOD QUESTION.
ALSO PROBABLY A HARD ONE TO ANSWER.
JUST BECAUSE EVEN AMONGST OUR PARTICIPANTS IT SEEMED
THEY WERE VARIED RESPONSES ON PEOPLES REACTION.
MOSTLY POSITIVE WHICH IS GOOD THIS.
WERE SOME PEOPLE THAT MENTIONED THEY DIDN'T
NECESSARILY TRUST THE PLATFORM ITSELF LIKE FACEBOOK.
THERE THEY DIDN'T TRUST WHATEVER THEY HAD TO SAY
ABOUT THE CORONAVIRUS.
MY SORT OF IMPRESSION THOUGH THAT IT'S BETTER THAT
THEY'RE DOING SOMETHING RATHER THAN NOTHING.

I THINK THAT ANY SORT OF FUTURE WORK IN THIS YEA AREA IS
TO LOOK AT THE OUT RIGHT DELETEING CORONAVIRUS
MISINFORMATION VERSUS JUST LABELING IT.
ALLOWING IT TO BE RESHARED.
RETWEETED.
LIKE THE GAMETE, YES.
>>
BUILDING ON THAT.
TAKING A STEP BACK FROM REMOVING A POEF.
IF I SEE FAULTS INFORMATION, DO THE PLATFORMS ALLOW
USERS TO POFT FOR FALSE INFORMATION OR IS IT GENERAL
ABUSE THE PLAT TOMORROWS HAVE
>> YES, TWITTER HAS A SPECIFIC MISINFORMATION LIKE
REPORTING LABEL.
I THINK FACE BOOK DOES AS WELL.
IT MOIETY BE A LITTLE MORE BROAD.
TWITTER ALLOWS YOU TO CHARACTERIZE IT BY POLL TECH,
ETCETERA, I WOULD LIKE TO DOUBLE CHECK.
THEY DO ALLOW REPORTING.
Y THOUGH IT'S UNCLEAR LIKE WHEN OR HOW THAT GETS
USED TO THE USE ARE.
>> HA MAKES SENSE.
TURNING BACK TO MARZ ISH EH.
IF YOU HAD TO FOCUS ON FISHING PREHAVINGS AND
PREHAVEN'TING PEOPLE FROM GETTING TO THE WOULD BE
SITES WHAT DO YOU THEUP YOU WOULD PRIORITIZE
>> IT'S IMPORTANT THAT ATTACKERS ARE SEVERAL STEPS
AHEAD OF MODERN PHISHING DEFENSES.
THEY TAKE ADVANTAGE OF GLOBAL DISASTERS TO HARM
USERS.
SO IT'S IMPORTANT TO SOLVE THE PROBLEM CO LAN ERA
COLLABORATIVELY.
MAYBE GO FURTHER AND HAVE A PROACTIVE DEFENSIVE
MECHANISM.
LIKE THIS IS THE MOST IMPORTANT THING.
I CAN'T EMPHASIZE HAVING PRACTICE WOULD HELP TO
T
PHISHING AND PROTECT USERS.
>> AND BUILDING ON THAT, REVOKEING CERTIFICATES
AFTER DISCOVERING WEB SITES.
>> THE THING IS AS I MENTIONED IT'S SOMETHING THAT
CAN BE DONE IN DIFFERENT STEP.
THAT'S WHY I SAID THE COLLABORATION.
THEY CAN PREVENT IT BOTH AT THE TIME OF

REGISTRATION.
IF THE REGISTERS CAN BE MORE CON SERVE TIFF OR CAUTIOUS.
ALSO SOMETHING TO FOCUS ON EVEN BEFORE AND AFTER THEY HAVE BEEN REPORTED.
SO, YES I THINK THAT'S SOMETHING THAT SHOULD BE DONE COLLABORATIVELY IN DIFFERENT STEPS TOO.
TO LIKE HAVE AN ACCEPTED RESULT.
>> ALRIGHT.
JUST AS A OVER ALL QUESTION FOR BOTH OF YOU.
DO YOU HAVE PLANS TO CONTINUE THIS WORK?
WHERE DO YOU SEE THIS GOING IN THE FUTURE?
CHRISTINE, I WILL START WITH YOU.
>> YA THAT'S A GOOD QUESTION.
WHAT I'M CURIOUS ABOUT IS THERE WAS A RECENT REPORT TALKING ABOUT HOW TO CATEGORIZE DIFFERENT INFORMATION CONSUMERS INTO DIFFERENT CATEGORIES LIKE PEOPLE WHO ARE SPECTACLE VERSUS THOSE WHO ARE NOT.
I WOULD BE REALLY INTERESTED IN SEEING HOW THAT RELATES TO THE EFFICACY OF LABELING A PLATFORM AS FALSE.
>> THAT WOULD BE INTERESTING.
I WOULD BE CURIOUS TO FIND OUT MORE AS WELL.
MARZIEH, I KNOW YOU TALKED ABOUT THE FRAUDULENT SITES.
DO YOU THINK FUTURE WORK WILL GO THAT WAY OR OTHER PLANS?
>> THE FUTURE WORK WE'RE LOOKING AT A EMPHASIS, LIKE WE KNOW ONE OF THE IMPORTANT STEP NEXT STEP WOULD BE TO IDENTIFY OTHER TYPE OF SCAM WEB SITES.
NOT ONLY FOR PHISHING AND TRY TO DETECT THEM AND PROTECT USERS FROM THE SCAMMER SITES.
THAT'S THE FUTURE DIRECTION FOR US.
>> THAT SOUNDS FASCINATING.
ALRIGHT.
TO WRAP UP I WOULD LIKE TO SAY THANK YOU VERY MUCH BOTH OF YOU FOR PRESENTING FOR US TODAY.
GREAT JOB EVERYONE.
THANK YOU, VERY MUCH.
I WILL PASS THIS OVER TO LERONE BANKS FOR CLOSEING COMMENTS.
§
>> TODAY WE HAVE HEARD FROM RESEARCHES ABOUT PRIVACY, RISKS, PRACTICAL METHODS CAN BE USED.

RESEARCHES PRESENTED WORK ON ANALYZING PRIVATE SEE POLICIES AND QUANTIFYING CONSUMER TRACKING.
THIS YEAR EASY VENT INCLUDED PANELS ON TIMELY PRIVACY ISSUES WITHIN THE CONTEXT OF IOT, TEAMS, THE PANDEMIC.
IT HAS BEEN A DAY FULL OF RESEARCH FULL OF DATA DRIVEN DECISION MAKING FOR THE FTC MISSION.
I WOULD LIKE TO EXPRESS GRATITUDE TO JAMIE HINE TO BRING THIS TO LIFE FOR THE SIXTH YEAR AND REITERATE HIS THANKS TO THE SUPPORTING TEAM, MODERATEERS AND RESEARCHERS FOR THEIR COMPELLING WORK.
I LOOK FORWARD TO EXPAND THE ROLL OF RESEARCH IN THE AGENCIES EVOLVING EFFORTS AS LAID OUT BY COMMISSIONER SLAUGHTER.
THANK YOU FOR ATTENDING PRIVACY CON2021.
SEE YOU NEXT YEAR.