FTC PrivacyCon
January 14, 2016
Segment 4
Transcript

>> WE'RE GOING TO GET STARTED IN

A COUPLE MINUTES HERE SO IF

PEOPLE COULD START GETTING BACK

TO THEIR SEATS, THAT WOULD BE

GREAT.

THANK YOU.

WE'LL WAIT A FEW MORE MINUTES

FOR PEOPLE TO GET BACK.

WELCOME BACK EVERYONE.

MY NAME'S KEVIN MORIARTY, I'M

WITH THE FEDERAL TRADES

COMMISSION.

THIS IS SESSION FOUR OF

ECONOMICS PRIVACY AND SECURITY.

WE HAVE PRESENTING A WEB

DISCOVERY ECO SYSTEMS.

SO WELCOME TO THE FIRST OF TWO

TALKS IN THIS SESSION THAT IS

ACTUALLY ABOUT SECURITY.

THIS IS JOINT WORK WITH OTHERS

AT THE COLLEGE OF INFORMATION

AND SCIENCE TECHNOLOGY AT PENN
STATE UNIVERSITY.
MY TALK IS ABOUT THE TOPIC OF
BOUNDARIES AND VULNERABLE
DISCOVERY THAT'S MOSTLY
CONDUCTED BY EXTERNAL
RESEARCHERS WE CALL WHITE HATS.
IN 1995, THE FIRST WUG BOUNTY
PROGRAM WAS FOUNDED BY NETSCAPE
THAT INVITED EXTERNAL SECURITY
RESEARCHERS TO SCRUTINIZE ITS
SERVICES.
SINCE THEN WE HAD A NUMBER OF
OTHER COMPANIES AND PROGRAMS
EMERGING THAT RUN IN AN
INDEPENDENT SESSION.
HOWEVER MORE RECENTLY WE
ACTUALLY OBSERVED THE EMERGENCE
OF SO-CALLED BUG COUNTY PLAT
HOMERS.
TWO OF THEM IS [INDISCERNIBLE]
WHICH IS THE FOCUS OF OUR STUDY.
JUNE WAS FOUNDED IN 2010 AND WAS

FOCUSED ON THE CHINESE MARKET.
IT OPERATES IN EUROPE AND IN THE
UNITED STATES MOSTLY AND WAS
FOUNDED IN 2007.
THE MOTIVATION FOR OUR STUDY IS
TO BETTER UNDERSTAND HOW THESE
WEB VULNERABILITY ECO SYSTEMS
ACTUALLY OPERATE AND WHETHER
THEY MAKE A SIGNIFICANT
CONTRIBUTION TO WEB SECURITY.
WE ALSO WANT TO PROVIDE USEFUL
DATA FOR THE POLICY.
FOR EXAMPLE ON THE LIMITS OF
VULNERABLE RESEARCH AND
PRACTICE.
OUR APPROACH IS TO DO AN
IN-DEPTH IMPEERITY STUDY OF THE
ECO SYSTEMS AND IN OUR PAPER WE
TAKE A BROAD APPROACH IN A SENSE
WE TRY TO UNDERSTAND
ORGANIZATIONS, WHITE HATS AND
BLACK HATS COULD PROBABLY
INTERACT ON THESE THIRD PARTY

VULNERABILITY PLATFORMS.

IN THE PRESENT AGENTS I WILL

MOSTLY FOCUS ON THE PERSPECTIVE

OF COMPANIES AND ORGANIZATIONS.

SO THE TWO PROGRAM THAT WE LOOK

AT HAVE A COUPLE COMMON ASPECTS.

MOSTLY THAT'S A VERY POPULAR.

A LIGHT OF SITES INTERACTING ON

THEM AND A LOT OF VULNERABLE

REPORTS ARE MADE BUT THERE ARE A

COUPLE IMPORTANT DIFFERENCES.

THE FIRST ONE IS THAT AN

ORGANIZATION INITIATED IN A

SENSE THAT THESE COMPANIES ASK

TO RUN A PARTICULAR PROGRAM FOR

THEM VERSUS [INDISCERNIBLE]

HACKERS REQUEST COMMIT ANY TYPE

OF VULNERABILITY OF ANY WEBSITE

ON A PLATFORM.

THIS IS DIFFERENT WITH RESPECT

TO THE BOUNTIES.

THE DIFFERENCE IS THE DELAY FOR

THE DISCLOSURE POLICY.

SO IRRESPECTIVE OF THE COMPANY
AFTER 45 DAYS THE WHOLE
TECHNICAL DETAILS OF DISCOVERED
VULNERABILITY WILL BE
COMMUNICATED TO THE PUBLIC.
THERE ARE SOME DIFFERENCES IN
THE TYPE OF DATA.
WE HAVE A LOT OF PLATFORMS SO WE
CANNOT ALWAYS COMPARE AND
CONTRAST THE TWO BUT WE CAN IN
BROAD CATEGORIES PROVIDE SOME
KIND OF COMPARISON ON HOW THESE
PLATFORMS PARTS OPERATE.
PARTICIPATION BY ORGANIZATIONS,
THE PUBLIC PROGRAMS THAT ARE RUN
IS LIMITED TO ABOUT A HUNDRED
AND ALL OF THOSE ARE I.T.
COMPANIES.
IN CONTRAST, MUCH BROADER
PORTFOLIO OF COMPANIES THEY ARE
MORE OR LESS OWE CURSED TO
PARTICIPATE ON THE PLATFORM.
AND INTERESTINGLY YOU SEE HERE A

LOT OF ORGANIZATIONS THAT
TYPICALLY ARE NOT KNOWN TO RUN
BOUNTY PROGRAMS BY THEMSELVES
LIKE GOVERNMENT INSTITUTIONS,
EDUCATION INSTITUTIONS AND
FINANCIAL INSTITUTIONS.
THE FIRST TAKE AWAY IS THE
INITIATED MODEL PROVIDES FOR
MUCH LARGER PARTICIPATE WHICH
MAY BE GOOD THAT SENSE OF WEB
SECURITY AS A MORE LIMITED
PARTICIPATION MODEL OF PLATFORM
SUCH AS HACKER ONE AND HOW THESE
PLATFORMS CAN ENCOURAGE MORE
COMPANIES TO PARTICIPATE.
A SECOND ISSUE WE WANT TO
EXPLORE IS EQUALITY OF THE
SUBMISSIONS AND WHAT WE OBSERVE
HERE, IN PARTICULAR ON THE
PLATFORM OF REGIME IS THAT WE
HAVE A VERY BROAD RANGE OF TYPES
OF VULNERABILITIES THAT ARE
SUBMITTED.

AND 44% OF THESE CASES, THESE
ARE ACTUALLY CLASSIFIED AS HIGH
SEVERITY VULNERABILITIES.
ON HACKER ONE THIS IS A LITTLE
BIT HARDER TO DETERMINE FROM
PUBLICLY AVAILABLE DATA.
HOWEVER IF YOU ACTUALLY PERUSE
THE BOUNTY AMOUNTS
[INDISCERNIBLE] LOOK INTO THE
POLICY STATEMENTS BY COMBINING
THESE TWO DATA POINTS WE CAN
ACTUALLY ALSO INFER HOW MANY
VULNERABILITIES OF HIGH AND
MEDIUM SEVERITY WHICH IS PLOTTED
ON THE SLIDE.
HERE WE CAN ALSO CONCLUDE ACROSS
THESE TWO PROGRAMS WHITE HATS
HAS MADE SIGNIFICANT
CONTRIBUTIONS TO THE SECURITY OF
THESE WEBSITES BY CONSULTANT
BOOTH -- CONTRIBUTING
SEVERITIES.
THE WHITE HAT INITIATED MODEL

THAT WE SEE SEEMS TO HAVE A
SMALL OF THESE VULNERABILITIES
IN A SUFFICIENT FASHION.
NOW THE QUESTION ARISES HOW WELL
ACTUALLY THESE DIFFERENT
PLATFORMS AND IN PARTICULAR THE
COMPANIES ASSOCIATED WITH THEM
CAN ACTUALLY RESPOND TO THESE
SUBMITTED VULNERABILITIES.
HERE WE SEE SOME INTERESTING
DIFFERENCES.
WHEN WE LOOK AT REGIME, ACTUALLY
SEE THAT IN PARTICULAR THOSE
VERY POPULAR COMPANIES AS
MEASURED BY, MEASURE THE AWE LEX
AWE RANK CAN RESPOND TO THE
VULNERABILITIES AND HANDLE THEM.
IN CONTRAST SMALLER WEBSITES IS
NOT CAPABLE TO DO SO.
IN FACT 25% OF THE SUBMITTED
VULNERABILITIES REMAIN ENTIRELY
UNHANDLED BY THE ORGANIZATIONS
TO WHICH THEY ARE TARGETED.

ON CONTRAST SINCE THESE ARE
INITIATED PROGRAMS WE SEE
RESPONSE TIME.
WITHIN FOUR AND-A-HALF HOURS WE
SEE A RESPONSE TO HAVE YOU BEEN
VUBLITIES AND MOST THEM HANDLE
IT WITHIN 30 DAYS.
AN INTERESTING TAKE AWAY ON THIS
WHITE INITIATED MODEL ON THESE
PLATFORMS WE SEE A LOT OF
COMPANIES THAT ARE COERCED TO
PARTICIPATE ARE ACTUALLY NOT
PREPARED WHICH IS SOMETHING THAT
WE HAVE TO TAKE INTO
CONSIDERATION.
VERSUS THAT OF COURSE RAISES A
QUESTION ON THE BALANCE SHOULD
WE ACTUALLY COERCE THESE
COMPANIES TO PARTICIPATE.
IS IT A REASONABLE ACTIVITY THAT
WE SHOULD BE ENGAGED IN.
THE NEXT QUESTION I'M
APPROACHING IS OF COURSE BROAD

INTAS.

WHAT IMPACT DO THESE KIND OF

BOUNDITIES HAVE.

HERE'S THE FIRST OVERVIEW THAT

WE ARE SEEING.

SO WHAT WE ARE SEEING HERE IS A

SUBSECTION OR SUBSAMPLE OF

COMPANIES PARTICIPATING IN

HACKER ONE.

WE SEE ON THE LEFT SIDE THAT

SOME COMPANIES ARE ACTUALLY NOT

PAYING ANY BOUNTIES AT ALL

VERSUS OTHERS WITH SUBSTANTIAL

BOUNTIES.

VULNERABILITIES ON AVERAGE THIS

DOESN'T HELP US TO DETERMINE

WHAT ACTUALLY WHAT THE

SIGNIFICANT IMPACT IS.

FOR THAT PURPOSE WE ACTUALLY

CONDUCTED THE REGRESSION

ANALYSIS IN WHICH THE DEPENDENT

VARIABLE IS A NUMBER OF

VULNERABLE SUBMITTED.

AND INDEPENDENT VARIABLES ARE
THE AVERAGE BOUNTY PAID BY A
PARTICULAR PROGRAM, THE
POPULARITY OF THE PROGRAM AND
THE MEASURE OF THE OVERALL
ACTIVITY OF THE WHITE HATS ON
THE PLATFORM IN A PARTICULAR
PERIOD.
SO WHAT WE ARE SEEING HERE IS
FIRST I WANT TO HIGHLIGHT THE
TOP PART OF THE TABLE IS THAT
ABOUT $100 INCREASE IN THE
EXPECTED BOUNTY PAY TOWARDS
WHITE HATS RESEARCHERS, WE SEE
ABOUT THREE MORE VULNERABILITIES
REPORTED TO THE PROGRAMS.
WHAT WE ALSO SEE IS THAT
PROGRAMS THAT ARE MORE POPULAR
ARE ALSO RECEIVING MORE
VULNERABILITY RECALLS.
THAT HAS TWO FACTOR.
ONE MORE POPULAR WEBSITES OF
COURSE RECEIVE MORE ATTENTION.

BUT OFTEN THEY ARE ALSO MORE
COMPLEX, OFFER MORE SERVICES TO
THE USERS SO THEY HAVE A LARGER
TEXT SURFACE IN THE SENSE FOR
WHITE HAT RESEARCHERS TO FIND
POTENTIAL VULNERABILITIES.
SO THE TAKE AWAY HERE IS THAT
WHITE HATS DO NOT NECESSARILY
ALWAYS FOCUS ON MONETARY
COMPENSATION.
IN FACT WHAT WE OBSERVED IS 20%
OF ALL CONTRIBUTIONS ON HACKER
ONE ACTUALLY GO TO THOSE
PROGRAMS THAT ACTUALLY DO NOT
PAY ANY BOUNTIES AT ALL.
SO PAY NOTHING ACTUALLY SERVES
AS A POTENTIALLY VIABLE
APPROACH.
IN CONTRAST WHAT WE ALSO OBSERVE
IS WELL, A HIGHER BOUNTY AMOUNT
AT THE END OF THE DAY IS STILL
ASSOCIATED ALSO WITH A LARGER
NUMBER OF HAVE YOU BEEN

VUBLITIES -- VULNERABILITIES
SUBMITTED BY THE WHITE HAT
RESEARCHERS.
IS LAST QUESTION THE ONE ABOUT
SECURITY IMPROVEMENTS.
WHAT DO WE ACTUALLY GET OUT OF
IT.
IN ORDER TO ASSESS IT, WHY WE DO
NOT HAVE AN INSIDE LOOK INTO THE
ORGANIZATIONS, WE ARE USING THE
TREND OF VULNERABILITIES
SUBMITTED OVER TIME.
SO THE ARGUMENT HERE IS IF YOU
HAVE DECLINING TREND OF
VULNERABILITIES EVERYTHING ELSE
KEEPING MODERATELY EQUAL, THEN
WE WOULD ARGUE PERHAPS AT THIS
PARTICULAR WEBSITE SECURITY'S
OVERALL IMPROVING.
WHEN YOU TAKE A FIRST LOOK AT
THE DATA YOU SEE IT'S ACTUALLY
RATHER SPIKY.
IT'S NOT IMMEDIATELY APPARENT BY

LOOKING AT THESE GRAPHICAL
DEPICTION WHAT KIND OF TRENDS
ARE EMERGING.
WHAT YOU SEE ON THE TOP THREE
GRAPHS FOR HACKER ONE IS
SEEMINGLY INITIAL SPIKE.
WHERE ONCE THE PROGRAM IS OPEN
ONE OF THE VULNERABILITY
RESEARCHERS ARE SUBMITTING THEY
HAVE STOCKPILED OR HAVE BEEN
ESSENTIALLY ENERGIZED BY THE
OPENING OF THE PROGRAM TO DO
IMMEDIATELY A LOT OF RESEARCH
THAT LED TO ADDITIONAL
SUBMISSIONS.
REGIME IS A LIT MORE NOISY TO
GET A BETTER UNDERSTANDING, WE
CONDUCT A STATISTICAL TEST,
ETCETERA CALLED A LA PAZ TREND
TEST AND WE FOCUS HERE ON
PROGRAM THAT HAVE A CERTAIN
AMOUNT OF MINIMUM ACTIVITY THAT
WERE RUNNING FOR AT LEAST FOUR

MONTHS, AT LEAST 50

VULNERABILITY REPORTS SUBMITTED

TO THEM.

WHAT WE SEE HERE IS ACTUALLY TWO

CONTRASTING TRENDS.

SO FOR HACKER ONE, WE ACTUALLY

OBSERVE THAT OVER TIME FOR THE

MAJORITY OF THE PROGRAMS WE SEE

AT DECREASING TRENDS OF

VULNERABILITY REPORTS, IN

CONTRAST FOR REGIME WHICH IS

INITIATED THIS COERCED

PARTICIPATION MODEL WE SEE

EXACTLY THE OPPOSITE.

MOSTLY AN INCREASE IN THE

VULNERABILITIES.

SO IF YOU REASON ABOUT THAT THEN

WE COULD ARGUE WELL DESPECIFIED

MONETARY OR PERHAPS BECAUSE

MONETARY INCENTIVES ARE IN

PLACE, WE ACTUALLY SEE

NEVERTHELESS THESE FEWER

VULNERABILITIES ON HACKER ONE.

SO DESPITE INCENTIVES, FEWER VULNERABILITIES WE ARGUE THIS IS INDICATIVE OF ACTUALLY IMPROVED WEB SECURITY PRACTICES AT THESE PARTICIPATING COMPANIES.

KEEP IN MIND AGAIN THESE PARTICIPATING COMPANIES ARE MOSTLY I.T. COMPANIES IN THE CASE OF THE PUBLIC HACKER ONE PROGRAMS.

WE ALSO SEE THIS INITIAL SPIKE WHICH FROM A WEB SECURITY POINT OF VIEW MIGHT BE REALLY WELCOME NEWS IF INDEED IT'S INDICATIVE, THAT'S A LOT OF THE STOCKPILED VULNERABILITIES ACTUALLY REMOVED FROM THE KNOWLEDGE OF WHITEHEAD AND POTENTIALLY BLACK HEAD.

WE SEE AN OPPOSING TREND FOR WOOYUN PROGRAMS AND OUR INTERPRETATION OF THAT IS THAT THIS LIKELY HAS TO DO SOMETHING WITH LACK OF PREPAREDNESS OF

THIS ORGANIZATIONS WHEN IT COMES
TO RECEIVING THESE VULNERABILITY
REPORTS.
FOR EXAMPLE THEY MAY NOT HAVE A
WELL DEVELOPED SECURITY SOFTWARE
DEVELOPING LIFE CYCLE, GOOD
INTEGRATION THAT MEAN THE
SECURITY TEAM AND THESE EXTERNAL
SECURITY DEVELOPERS AND MANY
OTHER FACTOR MIGHT ACTUALLY PLAY
A ROLE HERE.
WHICH ALREADY BRINGS ME TO THE
LAST POINT.
SO WE BELIEVE THAT IT'S
INSTRUCTIVE TO CONDUCT A REALLY
IN-DEPTH ANALYSIS OF THESE
PROGRAMS TO BETTER UNDERSTAND
WHAT CONTRIBUTIONS CAN WE
ACTUALLY MAKE TO THE OVERALL WEB
SECURITY AND PRACTICE.
AND IT'S DEFINITELY HELPFUL THAT
THESE TWO PROGRAMS PROVIDED US
WITH PUBLIC DATA WHICH WE CAN

STUDY IN DETAIL.

THERE ARE MANY MORE RESULTS

WHICH WE ACTUALLY HAVE ON A

PAPER IN PARTICULAR PERTAINING

TO HOW [INDISCERNIBLE] BEHAVE.

FOR EXAMPLE WE CAN SHOWCASE ON

PAPER HOW WHITE HEADS LEARN FROM

ONE ANOTHER BY INVESTIGATING THE

REPORTS OF THE$Jáx

ANOTHER, WE THE CAN ALSO STUDY

WHAT KIND OF DISCOVERY PATTERNS

THEY ACTUALLY HAVE IN PLACE, FOR

EXAMPLE, ARE THEY FOCUSING ON

SPECIFIC PROGRAMS OR ARE THEY

APPLYING THE SAME TYPE OF

TECHNIQUE ACROSS OTHER WEBSITES.

I ENCOURAGE YOU TO TAKE A LOOK

AT THEM.

IN TOTAL I BELIEVE THAT THE JURY

IS STILL OUT ABOUT WHICH OF

THESE TWO PARTICIPATION MODELS,

THE WHITEHAT INITIATED MODEL OR

THE COMPANY INITIATED MODEL ARE

REALLY BRINGING US THE BEST

ADVANTAGES.

ON THE FIRST GLANCE IT SEEMS

THAT THE WHITEHAT INITIATED

MODEL HAS BETTER PARTICIPATION,

MANY MORE ORGANIZATIONS THAT ARE

INVOLVED IN THESE KIND OF

ECOSYSTEMS.

BUT ON THE OTHER HAND A LOT OF

THESE PARTICIPATING

ORGANIZATIONS ARE NOT VERY WELL

PREPARED WHEN IT COMES TO

RECEIVING THESE KINDS OF

VULNERABILITY REPORTS AND

ACTUALLY THEN IMPROVING ALSO THE

SECURITY ON THEIR WEBSITES.

SO THERE ARE VARIOUS KINDS OF

PROS AND CONS WE CAN OFTEN, ONE

ISSUE IS CLEAR WE CAN JUMP START

OR FURTHER ENGAGE IN THE

DISCUSSION WHAT KIND OF

CONTRIBUTIONS OVERALL THESE

BOUNTY PROGRAMS MAKE TO THE

SECURITY OF THESE WEBSITES.

OUR INITIAL ASSESSMENT IS

POSITIVE BUT I THINK WE CAN GO

INTO FURTHER DETAIL DURING THE

DISCUSSION AND THIS BRINGS ME TO

THE END OF MY TALK.

THANK YOU VERY MUCH.

[APPLAUSE]

>> THANK YOU.

THANK YOU JENS.

NEXUS WE HAVE VERONICA MAROTTA

AND ALESSANDRO ACQUISTI FROM THE

CARNEGIE MELLON UNIVERSITY.

>> THANK YOU, THIS IS A JOINT

WORK BETWEEN VERONICA, C

CATHERINE AND MYSELF.

DECISIONS ABOUT PERSONAL

INFORMATION THE STUDY

REPRESENTED TODAY IS ALSO ABOUT

TRADITIONAL MICROECONOMICS AND

IT IS ABOUT UNDERSTANDING THE

ALLOCATIVE, TARGETED

ADVERTISING.

THERE IS STILL MOTIVATION IS
BEHIND OUR WORK, IN BEHAVIOR
DECISION RESEARCH IT IS VERY
WELL-KNOWN THAT HOW YOU FRAME A
CERTAIN PROBLEM, INFLUENCES THE
WAY PEOPLE WILL THINK ABOUT THIS
PROBLEM AND MAKE DECISIONS ABOUT
IT.
CURRENTLY WE LIVE NOT ONLY IN
THE AGE OF REAL DATA BUT UNDER
THE POWERFUL FRAME, THE FRAME
THAT PERSONAL DATA IS THE NEW
OIL AND WE'RE ALL GOING TO
BENEFIT PERHAPS IN EQUAL PARTS,
FROM SHARING PERSONAL
INFORMATION.
MORE SPECIFICALLY THERE ARE A
NUMBER OF FRAMES WHICH ARE QUITE
COMMON IN THE PUBLIC DEBATE OVER
PRIVACY.
PERSONAL INFORMATION IS THE LIFE
BLOOD OF THE INTERNET.
INCREASINGLY SOPHISTICATED

COLLECTION OF DATA IS NECESSARY
FOR US TO HAVE FREE SERVICES
ONLINE OR ALSO PRIVACY IS THE
PRICE TO PAY TO EXTEND THE
BENEFITS OF DATA, A WIN WIN
WHICH BENEFITS EQUALLY, OUR
BROAD RESEARCH AND AGENDA WE'RE
INTERESTED IN INVESTIGATING ALL
OF THESE FRAMES TO SEE HOW
ACTUAL EMPIRICAL EVIDENCE IS
SUPPORTING OR NOT SUPPORTING
THEM.
THE PAPER WE ARE PRESENTING
TODAY TACKLES THE LAST FRAME AND
MOST SPECIFICALLY RELATES TO THE
IMPACT THE TARGETED ADVERTISING
AS ON THE SURFACE OF DIFFERENT
STAKEHOLDERS.
CONSUMERS, ADVERTISING FIRMS AND
INTERMEDIARIES.
AND VERONICA WILL GUIDE YOU
THROUGH THE MODEL.
>> SO THANK YOU, ALESSANDRO.

>>> THE SPECIFIC RESEARCH
QUESTION WE ARE INTERESTED IN
ADDRESSING IS TO WHAT EXTENT THE
AVAILABILITY OF MORE AND MORE
PRECISE INFORMATION ABOUT
CONSUMERS IS TO AN INCREASING
TOTAL WELFARE, WHAT ALESSANDRO
JUST REFERRED THE AS THE
ECONOMIC WIN WIN VERSUS THE
CHANGE OF ECONOMIC BENEFITS
AMONG THE DIFFERENT STAKEHOLDERS
INCLUDING COMPANIES, CONSUMERS
AND INTO INTERMEDIARIES.
ALIGNED TARGETED ADVERTISING
THAT COMPARE DIFFERENT SCENARIOS
THAT DIFFER IN THE TYPE OF
CONSUMER INFORMATION THAT IS
AVAILABLE TO THE DIFFERENT
PLAYERS DURING THE TARGETING
PROCESS.
NOW SPECIFICALLY DIFFERENTLY
FROM PREVIOUS WORK WE ACCOUNT
FOR THE IMPORTANT ROLE PLAYED BY

THE INTERMEDIARY, AND WE FOCUS
ON A SPECIFIC MECHANISM, REAL
TIME BIDDING.
THE REAL TIMING I, LET ME
EXPLAIN YOU QUICKLY HOW IT
WORKS.
WE HAVE DIFFERENT PLAYERS
INVOLVED.
ON ONE SIDE, WE HAVE PUBLISHERS,
NAMELY WEBSITES THAT WISH TO
SELL ADVERTISEMENT SPACE THAT IS
AVAILABLE ON THEIR SITES.
ON THE OTHER SIDE WE HAVE
COMPANIES THAT WISH TO ADVERTISE
THEIR PRODUCTS ONLINE.
THOSE TWO PLAYERS DON'T NEED TO
COMMUNICATE DIRECTLY.
THEY CAN FACILITATE THE LOCATION
EVER ADVERTISEMENTS AND THE
TARGETING PROCESS.
SO THE MECHANISM WORKS AS
FOLLOWS.
WHEN A USER ARRIVES TO A

PUBLISHER'S SIDE, A SIGNAL IS
SENT THAT SINGLY BROADCASTED TO
COOKIES TO GEOLOCATIONS, AND USE
THE LOCATION FOR THE AUCTION OF
ADVERTISEMENT, ON THE BASIS OF
THE INFORMATION THE ADVERTISER
RECEIVES, THEY FORM A BID, HOW
MUCH THEY ARE WILLING TO PAY TO
THE USER AND COMMONLY THE CHANGE
USES CERTAIN COMPRISEAUCTION.
HE PAYS THE SECOND HIGHEST BID,
SO ONCE THE BID, THE WINNER IS
DETERMINED HE'S ALLOWED TO SHOW
THE ADVERTISEMENT TO THE USER.
NOW ON THE BASIS OF THIS
MECHANISM, WE BUILD A MODEL THAT
FOCUSES ON THE INTERACTION AMONG
THREE MAIN PLAYERS, THE
ADVERTISERS, THE INTERMEDIARY
AND THE CONSUMER.
THEY WANT TO ADVERTISE THEIR
PRODUCT TO THE CONSUMERS THAT
THEY WILL LIKE AND THEREFORE BUY

THEIR PRODUCT.

NEVERTHELESS THEY CANNOT CONTACT

CONSUMERS DIRECTLY.

WE ASSUME THAT THE INTERMEDIARY,

PRODUCT PROCESS THEY NEED TO

KNOW WHICH SELLER IS SELLING THE

PRODUCTS.

PLAYS AN INFORMATIVE ROLE,

FURTHER, WE ASSUME THAT THE

CONSUMER CAN BE CATEGORIZED, BY

HORIZONTAL INFORMATION, AND

VERTICAL INFORMATION CAPTURING

DIFFERENCES IN PURCHASE POWER.

NOW, THESE THREE PLAYERS

INTERACT IN OUR MODEL IN THIS

WAY.

AT THE GIVEN POINT IN TIME, A

CONSUMER IS ONLINE, AND HE MAY

BE CHARACTERIZED BY THESE TWO

PIECES OF INFORMATION,

HORIZONTAL AND VERTICAL.

THE OTHER CHANGE RECEIVE THE

SIGNAL ABOUT A CONSUMER,

INFORMATION AND HOLDS AN AUCTION
FOR THE LOCATION OF AN
ADVERTISEMENT TO THE CONSUMER.
ON THE BASIS OF THE INFORMATION
THEY RECEIVE OTHER ADVERTISERS
FORM A BID.
THE AUCTION IS RUN, THE WINNER
IS DETERMINED AND IT IS ALLOWED
TO SHOW THE ADVERTISEMENT TO THE
CONSUMER.
THE CONSUMER SEES THE
ADVERTISEMENT AND MAKES HIS
PURCHASE DECISION.
IT SHOULD BE CLEAR THAT THE
OUTCOME OF THIS PROCESS
CRUCIALLY DEPENDS ON THE
INFORMATION AVAILABLE DURING THE
TARGET PROCESS.
THEREFORE, WE UNDERSTAND HOW THE
INFORMATION CHANGES WHEN
DIFFERENT TYPES AND AMOUNTS OF
THE CONSUMER'S INFORMATION ARE
AVAILABLE.

WE CONSIDER SPECIFICALLY FOUR
CASES.
A CASE WHERE ONLY THE HORIZONTAL
INFORMATION IS AVAILABLE, A CASE
WHERE ONLY THE VERTICAL
INFORMATION IS AVAILABLE, A CASE
WHERE BOTH PIECE IS OF
INFORMATION ARE AVAILABLE, AND A
BENCHMARK CASE WHERE NO
INFORMATION ABOUT CONSUMERS IS
AVAILABLE, SO AN EXTREME FULL
PRIVACY CASES.
FOR EACH OF THESE CASES WE
ARRIVE AT WHAT THE FORM'S BEST
STRATEGY AND THEREFORE WHAT THE
FIRM'S PROFIT, WHAT IS THE
INTERMEDIARY PROCESS.
I WILL NOT GO THROUGH THE
MATHEMATICS OF THE MODEL BUT
SHOW YOU INTERESTING RESULTS
THAT WE OBTAINED BY SIMULATING
THE MODEL.
WHAT WE DO WE ARE ON

COMPUTATIONAL SIMULATIONS TO
ANALYZE THE OUTCOME IN TERMS OF
CONSUMER SURPLUS, INTERMEDIARY
PROFIT AND, IN THE FOUR
DIFFERENT INFORMATIONAL
SCENARIOS.
LET ME START FROM THE CONSUMERS.
NOW, THE GRAPHIC YOU SEE HERE,
THE X AXIS CAPTURES HOW
HETEROGENEOUS CONSUMERS ARE IN
THEIR PREFERENCES.
WHY THE Y AXIS, LOW VALUES MEANS
HIGH HETEROGENEITY.
THE DIFFERENT COLORS CORRESPONDS
TO THE DIFFERENT SCENARIOS THAT
WE CONSIDER.
SPECIFICALLY EACH REGION
CAPTURES UNDER WHICH SCENARIOS
THE CONSUMERS ARE BETTER OFF.
SO WE HAVE TWO PREDOMINANT
COLORS HERE.
THE GREEN REGIONS CAPTURES ALL
THE COMBINATIONS THE MODEL

PARAMETERS FOR WHICH CONSUMERS
ARE BETTER OFF, WHEN ONLY THE
HORIZONTAL INFORMATION IS
AVAILABLE DURING THE TARGETING
PROCESS.
SO WHAT'S THE INTUITION THERE?
IN THEIR REGION CONSUMERS ARE
MORE HETEROGENEOUS IN THEIR
PRODUCT PREFERENCES.
ACTUALLY ENSURES THE CONSUMERS
SEE THE ADVERTISEMENTS FOR THE
PRODUCTS THEY LIKE THE MOST.
SO THERE IS A BETTER MATCHING
BETWEEN CONSUMERS AND COMPANIES.
THE YELLOW REGION INSTEAD
CAPTURES ALL THE COMBINATIONS OF
MODEL PARAMETERS UNDER WHICH THE
CONSUMERS ARE BETTER OFF, WHEN
KNOWN INFORMATION ABOUT THEM IS
REVEALED.
IN THEIR REGION CONSUMERS TEND
TO BE MORE HOMOGENEOUS.
SO BRANDS DON'T MATTER AS MUCH.

SO THE TARGETING IS NOT AS
AVAILABLE TO CONSUMERS.
WE CAN CONSTRUCT A SIMILAR GRAPH
FOR INTERMEDIARY PRODUCE.
COMBINATION FOR MODEL
PARAMETERS, WHEN KNOWN
INFORMATION IS REVEALED ABOUT A
CONSUMER.
SO WE SAID THE REGION CONSUMERS
TEND TO BE MORE HOMOGENEOUS.
SO WHAT HAPPENS IS THAT IF
ADVERTISER HAD THAT INFORMATION,
THEY WILL TEND TO BID LOWER TO
SHOW THE ADVERTISEMENT, LOWER IN
THE INTERMEDIARY'S PROFIT.
IF THE INFORMATION IS NOT
REVEALED THEN THE ADVERTISERS
HAVE TO BID IN EXPECTATION SO
THEY MAY OVERBID INCREASING THE
INTERMEDIARY'S PROFIT.
THE RED REGION INSTEAD IS THE
COMBINATION OF MODEL PARAMETERS
FOR WHICH THE PROFITS DESIRED,

WHEN THE VERTICAL INFORMATION IS
AVAILABLE.
IN THE REGION CONSUMERS ARE MORE
HETEROGENEOUS, SO REVEALING THE
VERTICAL INFORMATION DURING
TARGETING PROCESS INTENSIFIES
THE COMPETITION AMONG THE
BIDDERS.
THEY MAY TEND TO BID MORE
AGGRESSIVELY.
IF WE PUT TOGETHER THESE TWO
PICTURES, WE HAVE SITUATIONS IN
WHICH THE INTEREST OF THESE TWO
PLAYERS ARE ACTUALLY ALIGNED.
SEE THE YELLOW REGION.
BUT THERE ARE ALSO SITUATIONS IN
WHICH THEY HAVE CONTRASTING
INTEREST.
SO LIMITING CONSIDERATION OF AN
INTERMEDIARY THAT MAY HAVE POWER
OVER THE INFORMATION ABOUT A
CONSUMER, AND MAY DECIDE TO ACT
STRATEGICALLY, EITHER BY

REVEALING THEIR OWN INFORMATION,
SEE GREEN VERSUS RED REGION OR
REVEALING TOO MUCH INFORMATION
WHEN INSTEAD CONSUMERS WOULD
HAVE BEEN BETTER OFF WHERE LESS
INFORMATION WOULD HAVE BEEN
REVEALED.
TO UNDERSTAND AND ANALYZE HOW
THE ALLOCATION OF THE BENEFITS,
CHANGES UNDER THE AREAS, WE CAN
CONSTRUCT A BUY CHART LIKE THE
ONE WE ARE SEEING NOW FOR AN
INFORMATION CASE WHERE WE SEE
THE PERCENTAGE OF THE VALUE
GENERATED TO A TARGETING PROCESS
THAT IS CAPTURED BY EACH PLAYER.
SO WE CAN HAVE A PIE CHART FOR
EACH SCENARIO, AND WHAT THIS PIE
CHART SHOWS IS ACTUALLY A
PATTERN VERY SIMILAR TO WHAT WE
JUST DISCUSSED.
CONSUMERS IN BLUE TEND TO BE
BETTER OFF EITHER IN THE NO

INFORMATION CASE OR ON THE
HORIZONTAL INFORMATION CASE.
WHERE INTERMEDIARY IN RED SEEMS
TO CAPTURE A LOT OF BENEFITS
WITH THE VERTICAL INFORMATION
ONE BEING BY FAR THE BEST CASE.
FOR INSTEAD INTUITIVELY IT IS
BETTER AT LEAST TO HAVE SOME
INFORMATION ABOUT THE CONSUMERS
WITH A COMPLETE INFORMATION CASE
BEING IN THIS CASE IS BEST
SCENARIO.
SO IF YOU WANT TO SUMMARIZE
THOSE FINDINGS WE FIND THAT
CONSUMERS ARE GENERALLY BETTER
OFF EITHER WHEN SPECIFIC TYPE OF
INFORMATION ABOUT THEM ARE
AVAILABLE, OR IN GENERAL, WHEN
LESS INFORMATION IS AVAILABLE,
AND THERE ARE SITUATIONS WHERE
THE INTEREST OF THE PLAYERS SEE
INTERMEDIARY AND CONSUMERS SEEM
A-- ALIGNED.

IN ORDER TO MAXIMIZE ITS PROFIT.

SO I'LL LEAVE ALESSANDRO TO DO

SOME FINAL REMARKS.

>> THANK YOU.

THERE ARE A NUMBER OF EXTENSIONS

WE ARE PLANNING OR WORKING ON.

PROBABLY THE MOST IMPORTANT IS

THE EMPIRICAL VALIDATION.

IN FACT IF REPRESENTATIVES OF

NETWORKS ARE IN THE ROOM OR

FOLLOWING VEE THE WEBCAST -- VIA

THE WEBCAST, IF YOU WANT TO

PROVE OR DISPROFFER THE PROCESS

WE ARE HAPPY TO WORK WITH YOU.

OT THE LEFT YOU HAVE THE THREE

FRAMES I STARTED FROM, AND I

CLAIM THAT IS IN COMMON, VERY

LITTLE EMPIRICAL VALIDATION.

I'M NOT CLAIMING THEY ARE

NECESSARILY WRONG, I'M CLAIMING

WE DON'T KNOW REALLY HOW TREE

TRUE THEY ARE.

ON THE RIGHT I HAVE THREE BROAD

QUESTIONS THAT ARE IMPORTANT TO
UNDERSTAND DATA IS THE NEW OIL
AND TO WHAT BENEFITS THE NEW OIL
ARE ALLOCATED TO THE DIFFERENCE.
HOW IS THE SURPLUS GENERATED, TO
FIND A NICE COMBINATION OF
PROTECTION OF DATA AND SHARING
DATA, ARE THERE COSTS AND IF SO
WHO IS SUFFERING THOSE COSTS?
INDIVIDUAL CONSUMERS BECAUSE
THEY MAY GET LESS TARGETED
ADVERTISING, SOCIETY AS A WHOLE
BECAUSE MAYBE THE NEXT MEDICAL
RESEARCHER INVESTIGATING CANCER
CAN'T GET ENOUGH DATA OR JUST
THE ISSUE OF INCREASING THE RENT
EXTRACTED BY OLIGOPOLIES.
AND VERY DIFFERENT POLICY
CONCLUSIONS AND FINALLY IN
WHAT -- UNDER WHAT CONDITIONS TO
CONSUMERS BENEFIT FROM TRADING
CERTAIN DATA AND WHAT CONDITIONS
THEY DO NOT?

I BELIEVE THE ANSWER IS NOT

BINARY, IS CONTEXT DEPENDENT.

THIS IS WORK IN PROGRESS.

IN FACT IS WORK IN OUR AGENDA.

HOWEVER IF YOU ARE INTERESTED IN

THE CROWN MATERIAL IN THIS AREA

AND BY THIS AREA I MEAN THE

ECONOMICS OF PRIVACY YOU CAN

FIND ON SSRN A SEMI-FINAL

VERSION OF A PAPER THAT CURTIS

TAYLOR, LEA WAGMAN AND MYSELF

HAVE SUBMIT, WE WILL LEAVE WITH

YOU THIS THANK YOU VERY MUCH FOR

YOUR ATTENTION.

[APPLAUSE]

>> THANK YOU VERONICA AND

ALESSANDRO.

NEXT IS CATHERINE TUCKER FROM

M.I.T.

>> THANK YOU VERY MUCH FOR

HAVING ME.

I'M CATHERINE TUCKER ANDI'M A

ECONOMIST WHO STUDIES THE

ECONOMIC FEKS OF ARE PRIVACY
INFORMATION USING REAL LIFE DATA
ACCOUNT.
WHAT I'M GOING TO BE PRESENTING
TODAY IS INFORMATION FROM AMALIA
MILLER, CONSUMER TAKEUP OF
GENETIC TESTING.
I KNOW A LOT OF YOU ARE HERE TO
THINK ABOUT ECONOMIC DATA AND
TESTING.
WHY WE THINK IT WAS INTERESTING
IS THAT FIRST OF ALL THIS IS A
TECHNOLOGY WITH A HUGE UPSIDE AS
I'LL GET OLATER.
SECONDLY IT IS ALSO A TECHNOLOGY
WHERE I THINK EVEN THE MOST
CYNICAL PERSON ABOUT PRIVACY
WOULD SAY THERE ARE POTENTIAL
PRIVACY CONSEQUENCES OF THIS
DATA BEING CREATED.
SOMETIMES WHEN YOU'RE THINKING
ABOUT TARGETED ADVERTISING IT IS
HARD TO ACTUALLY ARTICULATE A

PRIVACY FIRM WHICH IS OFTEN WE
THINK ABOUT HEALTH AND FINANCIAL
EXAMPLES.
BUT GENETIC DATA IT'S NOT HARD
TO COME UP WITH EXAMPLES OF
HARM.
FOR EXAMPLE I TOOK A 23 AND ME
TEST.
DEPRESSING I GOT A THREE TIMES
AVERAGE TIME OF GETTING MACULAR
DEGENERATION, WHICH MEANS I
WON'T SEE TOO WELL.
I FEEL CONFIDENCE ANNOUNCING IT
IN THIS AUDIENCE, I PROBABLY
HAVE THE LEAST POTENTIAL
CONSEQUENCE HE OF ANYONE IN THE
WORLD OF RELEASING THIS DATA,
BECAUSE I HAVE A JOB AND I HAVE
HEALTH INSURANCE.
THERE IS POTENTIAL, YOU CAN'T GO
FAR WITHOUT THINKING OF
POTENTIAL NEGATIVE CONSEQUENCES
OF THAT DATA.

AND AS THE PREVIOUS GENERATION
OF GENETIC PRIVACY ARTICULATED
VERY WELL, THERE ARE ISSUES OF
IDENTIFIABILITY.
THE FACT THAT THIS DATA IS
PERSISTENT.
AND THE FACT THAT POTENTIALLY
THIS DATA HAS SPILLOVERS TO
FAMILY MEMBERS SO PRIVACY
CONSEQUENCES THAT ARE
SIGNIFICANT.
THE REASON I THINK THIS PAPER
SETTING WAS USEFUL IS SIMPLY
BECAUSE THERE HAS BEEN A LOT OF
EXPERIMENTATION THAT ALLOWS US
TO HAVE MORE OF A HORSERACE THAN
WE USUALLY DO, WHEN WE SEE HOW
PRIVACY OPTIONS WORK.
HUGE UPSIDE, AND THE UPSIDE IS
THE PROMISE OF PERSONALIZED
MEDICINE.
AND THE TYPICAL STATEMENT MADE
IN FAVOR OF PERSONALIZED

MEDICINE IS FOR THE AVERAGE DRUG
BASED ON YOUR GENETIC MAKEUP IT
WON'T WORK 25% OF THE TIME.
SO WE CAN IMAGINE IF WE ACTUALLY
HAD GENETIC DATA WE WILL BE ABLE
TO IDENTIFY POTENTIAL DRUGS AND
SAVE MONEY AT THE SAME TIME.
I FIND IT USEFUL TO BRING IT TO
LIFE WITH A VERY PERTINENT
EXAMPLE WHICH IS THE EXAMPLE OF
ANGELINA JOLIE.
SHE DID GENETIC TESTING, SHE
FOUND OUT THAT SHE UNFORTUNATELY
HAD A MUTATION IN HER GENES THAT
SHE WAS LIKELY TO GET BOTH
BREAST AND OVARIAN CANCER AND AS
A RESULT HAD A DOUBLE MASTECTOMY
AND HYSTERECTOMY.
THIS IS OBVIOUSLY A STRIDENT AND
DECISIVE MEDICAL ACTION BUT IN
PRINCIPLE IT'S GOING TO REDUCE
HER CHANCE HE OF GETTING CANCER
BY 70%.

-- CHANCES OF GETTING CANCER BY 70%.

THIS IS DATA WHICH LEADS TO EXTREME FORMS OF ACTION IN A MEDICAL SENSE BUT HUGE UPSIDE IN HEALTH OUTCOMES IN TERMS OF IT BEING CREATED.

NOW WHAT WE'RE GOING TO DO IN THIS STUDY IS LOOK AT STATE LAWS EXPERIMENTATION WITH DIFFERENT TYPES OF PRIVACY REGULATION FROM 2000 AND 2010.

AND WHAT'S NICE ABOUT THIS VARIATION IS YOU ALWAYS WORRY IN ANY EMPIRICAL STUDY WHERE THE VARIATION IS COMING FROM, WHY ARE THE STATES ACTUALLY EXPERIMENTING IN THIS WAY AS AN UNDERLYING REASON.

FROM WHAT WE CAN SEE IT WAS PRETTY RANDOM DRIVEN BY INDIVIDUAL STATE SENATORS WHO GOT A BEE IN THEIR BONNET.

WHAT IS ALSO NICE IS THEY ARE
EXPERIMENTING WITH MANY
DIFFERENT TYPES OF PRIVACY
REGULATION AND WE ARE GOING TO
BUCKET THEM INTO THE STUDY INTO
FREE BUCKETS WHICH ARE INFORMED
CONSENT, REGULATING DATA USE AND
ESTABLISHING PROPERTY RIGHTS.
AND I WANT TO IN THE PAST WHAT
I'VE DONE IS I'VE SAID WELL YOU
KNOW THE GREAT THING ABOUT THIS
IS IT ACTUALLY EMULATES
DIFFERENT COUNTRIES' APPROACHES
TO DOING PRIVACY REGULATION, IF
YOU TAKE EU AND OECU APPROACHES,
INFORMED CONSENT, MAYBE THE U.S.
WE THOUGHT ABOUT RESTRICTING
DATA USE AND THIS ECONOMIST
DREAM OF ESTABLISHING PROPERTY
RIGHTS.
NOW I SAY I'VE SAID THAT IN THE
PAST.
THE REASON I NO LONGER PUSH IT

IS I MENTIONED THIS ONCE WHEN I
WAS GIVING THIS TALK IN PARIS,
AND THIS PERSON FROM THE
MINISTRY OF CULTURE IN FRANCE
STOOD UP AND SAID HOW DARE YOU
SAY THAT.
IN FRANCE WE REGULATE PRIVACY IN
EVERY SINGLE WAY YOU COULD
POSSIBLY IMAGINE SO IT'S NOT
JUST ONE.
BUT IN GENERAL, WHAT'S NICE
ABOUT IT IS AT LEAST WE GOT A
HORSERACE FOR DIFFERENT WAYS WE
MIGHT THINK ABOUT REGULATING
PRIVACY.
NOW, WE'RE GOING TO HAVE DATA ON
PEOPLE'S DECISIONS TO GET THESE
GENETIC TESTS.
WE'RE LUCKY WE HAVE A NATIONAL
SAMPLE THAT WAS DONE EVERY FIVE
YEARS IN THE PEER WE'RE STUDYING
AND THEY'RE GOING TO BE ASKING
30 THOU PEOPLE ABOUT WHETHER OR

NOT THEY HAD A GENETIC TEST IN
EACH SAMPLE.
NOW, IT'S A GREAT DATA SET IN
ONE WAY.
AND THEY FOCUS ON THE DECISION
TO GET A GENETIC TEST FOR
WORKING OUT WHETHER OR NOT YOU
HAVE GENETIC SUSCEPTIBILITY
TORTS BREAST OR OVARIAN CANCER.
THE REASON I SAY THIS IS A VERY
INTERESTING GENETIC TEST IS IT'S
SOMETHING YOU CAN DO WITH THIS
INFORMATION TO SAVE YOUR LIFE IF
YOU TAKE THE TEST.
SO POTENTIALLY, THIS IS A HUGELY
VALUABLE HEALTH -- PIECE OF
HEALTH DATA TO CREATE.
NOW, THE NEGATIVE IS, THAT THIS
IS A TECHNOLOGY IN ITS EARLY
STAGES AND SO AS A RESULT, WE'RE
ONLY SEE A LITTLE BIT OF TAKEUP
IN OUR SAMPLE, ABOUT LESS THAN
1%.

NOW, WHAT WE'RE GOING TO DO IN
THE PAPER IS USE STANDARD
ECONOMETRIC TECHNIQUES, OF THESE
PEOPLE THIS OUR SAMPLE TO GO AND
GET A GENETIC TEST TO WHAT THE
STATE PRIVACY REGIME WAS LIKE IN
THAT PARTICULAR YEAR.
NOW, I REALIZE THIS IS NOT AN
ECONOMIST AUDIENCE, SO WHAT I
WANT YOU TO THINK OF THIS IS THE
STATISTICAL RELATIONSHIP THAT WE
DO WHERE WE'RE CONTROLLING FOR
JUST ABOUT EVERYTHING THAT YOU
MIGHT THINK OF GOING ON IN THE
BACKGROUND.
WE ARE CONTROLLING FOR THE YEAR.
WE'RE CONTROLLING FOR THE STATE.
WE'RE CONTROLLING FOR EVERYTHING
ABOUT THE PATIENT.
NOW, IF YOU LIKE EQUATIONS AND
SUBSCRIPTS, THE PAPER'S GOT
PLENTY OF THOSE SO I DIRECT
THROUGH.

NOW FOR THIS AUDIENCE WHAT I
DECIDED TO DO IS TO PRESENT THE
MAIN RESULTS IN A BAR CHART.
AND THE BIG PUNCH LINE IS, THAT
WE BUCKET UP OUR STATE
REGULATIONS IN THIS WAY.
WHAT WE FIND IS THAT WHEN YOU
HAVE INFORMED CONSENT, AND
THAT'S INFORMED CONSENT WHERE
WE'RE TELLING PEOPLE HOW THE
DATA'S GOING TO BE USED, WE GET
A REDUCTION OF THIRD OR IN TERMS
OF HOW MANY PEOPLE ARE TAKING A
GENETIC TEST.
NOW, THIS IS A LARGER PORTION
BUT REMEMBER THESE ARE QUITE
SMALL NUMBERS.
SO THE BASELINE IS SMALL.
NOW, WHEN WE HAVE A USAGE
RESTRICTION, THAT IS WE SAY, OR
THE STATE GOVERNMENT SAYS THIS
DATA CAN'T BE USED TO
DISCRIMINATE, SAY BY EMPLOYER,

SAY BY HEALTH INSURANCE
COMPANIES, THAT REALLY HAS NO
STATISTICAL EFFECT THAT WE CAN
MEASURE.
THE THING WHICH HAS THIS BIG
BOOST OR POSITIVE EFFECT ON THE
DECISION TO GET A GENETIC TEST
IS WHETHER OR NOT YOU ACTUALLY
GIVE INDIVIDUALS CONTROL OVER
HOW THAT DATA WILL BE USED IN
THE FUTURE.
NOW, WHETHER YOU GET RESULTS
LIKE THIS, AS AN ECONOMIST
YOU'RE ALWAYS GOING TO WONDER
WHERE ARE THEY COMING FROM AND
WHAT'S THE EXPLANATION.
ONE THING THAT WORRIED ME IS
IT'S NOT ABOUT THE PATIENTS,
MAYBE IT'S ABOUT HOSPITALS AND
WHETHER OR NOT THEY ARE OFFERING
THE TESTS.
WE COLLECTED MORE DATA TO TEST
THIS AND WE FOUND THAT'S REALLY

NOT THE EXPLANATION.

IT IS THE CASE THAT IF YOU HAVE

THESE CONSENT LAWS HOSPITALS

REACT NEGATIVELY.

THAT'S NOT A SURPRISE.

I FOUND THAT IN THE PAST.

BASICALLY IT'S BECAUSE YOU HAVE

TO CONSTRUCT AN ENTIRE PARALLEL

SYSTEM.

HOWEVER WHAT WAS IMPORTANT ABOUT

THIS STUDY WAS WE DIDN'T FIND,

WHAT WE FOUND WAS A NEGATIVE

REACTION BY HOSPITAL HE IN TERMS

OF WHETHER THEY OFFER GENETIC

TESTS TO GIVEN PATIENTS PROPERTY

RIGHTS.

AGAIN MAYBE NOT SURPRISING WHY

WOULD YOU SET UP A GENETIC

TESTING FACILITIES OF YOUR

HOSPITAL, PROBABLY TO DO SOME

RESEARCH AND THIS IS GOING TO

RESTRICT YOUR ABILITY TO DO

RESEARCH BUT IT SUGGESTS THAT

THE MAIN EFFECT OF HAVING THESE
INDIVIDUAL CONTROLS POSITIVELY
AFFECTING OUTCOMES IS NOT DRIVEN
BY THE SUPPLY SIDE, BUT INSTEAD
DRIVEN BY PATIENTS.
NOW, MORE PROOF OF THIS IS WHAT,
AGAIN, TYPICAL THING WE WOULD DO
IN THE ECONOMICS, THAT WE'RE
ALWAYS GOING TO WORRY ABOUT
WELL, YOU SAY IT'S ABOUT
PATIENTS BUT COULD THERE BE
ANOTHER EXPLANATION OF SOMETHING
ELSE GOING ON IN THE STATE?
WE TESTED FOR THIS BY LOOKING AT
ALTERNATIVE EXPLANATIONS.
ONE SUCH TEST WAS, WE LOOKED TO
SEE WELL, IF WE LOOK AT THE
DECISION TO HAVE AN HIV TEST,
WHAT YOU MIGHT SEE, THINK OF IS
SIMILARLY SENSITIVE OHAVING A
GENETIC TEST, COULD WE SEE ANY
INFLUENCE OF THE GENETIC LAWS ON
THAT DECISION?

WE FOUND ABSOLUTELY NOTHING.

WE SUGGEST IT'S NOT DRIVEN BY

UNDERLYING TASTES OR PRIVACY IN

THAT STATE.

SIMILARLY WE COULDN'T FIND

GENETIC LAW EFFECTS ON FLU

SHOTS, WHICH SUGGESTS IT'S NOT

DRIVEN BY TASTE FOR PREVENTATIVE

CARE.

WHAT'S REALLY GOING ON?

I'VE RULED OUT HOSE, I'VE RULED

OUT SPURIOUS CONSULTATION TO DO

WITH THE STATE.

I THINK WHAT WE'RE GOING TO

ARGUE IS THAT ULTIMATELY IT

MAKES SENSE WHEN YOU UNDERSTAND

HOW THIS PRIVACY INFORMATION IS

DELIVERED.

GENETIC TESTING IS UNUSUAL IN

THAT YOU HAVE GENETIC COUNSELING

WHERE YOU SIT DOWN FOR GENETIC

COUNSELOR AND YOU WILL DISCUSS

THESE PRIVACY POLICIES FOR

PERHAPS 20 MINUTES AS WELL AS
THE POSITIVE AND NEGATIVE
CONSEQUENCES OF TAKING A TEST.
SO THIS IS VERY DIFFERENT FROM
THE TYPICAL ONLINE ENVIRONMENT.
WE KNOW THAT CONSUMERS ACTUALLY
FIND OUT ABOUT SOME OF THESE
LAWS.
THE LAWS THEY DON'T FIND OUT
ABOUT, THOUGH, ARE THE
ANTIDISCRIMINATION LAWS.
THESE AREN'T USUALLY PART OF THE
CONVERSATION.
AND I THINK THAT SPLAIBS REALLY
WHAT THE -- EXPLAINS REALLY JUST
THE LACK OF EFFECT, CONSUMERS
AREN'T REALLY CONCERNED BECAUSE
THEY DON'T FIND OUT ABOUT THESE
LAWS EXISTING.
ON THE OTHER HAND, WHEN YOU GO
THROUGH THE TYPICAL FORMS OR
PROCESS WHEN SOMEONE IS GIVEN
INFORMED CONSENT AND TOLD HOW

THE DATA IS BEING USED BUT NOT
CORRESPONDINGLY GIVEN CONTROL,
WE ARE GOING TO HIGHLIGHT THE
SENSE OF POWERLESSNESS WHICH CAN
PERHAPS EXPLAIN SOME OF THE
NEGATIVE EFFECTS.
WHEREAS WHEN YOU RESTORE CONTROL
TO THE PATIENT OVER HOW THEIR
DATA MIGHT BE USED IN THE FUTURE
THEN WE HAVE RECEPTION OF
CONTROL AND POTENTIALLY A
POSITIVE EFFECT WHICH MIGHT
ENCOURAGE THEM TO GO AHEAD WITH
THE TEST.
NOW, WE HAVE SOME MORE MATERIAL
IN THE PAPER WHERE WE TRY AND
PROVE THAT THIS REALLY IS ABOUT
PRIVACY CONCERNS IN THAT WE SHOW
THAT THESE EFFECTS ARE GOING TO
BE HIGHER IN SITUATIONS WHERE
THERE'S MORE LIKELY TO BE BAD
NEWS IF YOU HAVE A GENETIC TEST,
THAT ISSUES A REASON TO THINK

YOU'RE GOING TO HAVE BAD

INFLUENCES FROM THE TEST.

HOWEVER WE ALSO SHOW THERE'S

ABSOLUTELY NO EFFECT IF YOU HAVE

ALREADY GOT BAD NEWS.

THAT IS, IF YOU ALREADY HAVE

CANCER, THE BAD NEWS IS OUT

THERE IN YOUR RECORD AND NONE OF

THESE PRIVACY ISSUES ARE GOING

TO DRIVE ANY OF THE EFFECTS.

WE ALSO SHOW THAT THE EFFECTS

ARE LARGEST FOR PEOPLE IN THE

SURVEYS WHO TOOK VARIOUS PRIVACY

PROTECTING ACTIONS SUCH AS

REFUSING TO STATE INCOME.

SO AGAIN THAT'S GOING TO DRAW IT

BACK TO PRIVACY RATHER THAN

SOMETHING ELSE EXPLAINING MY

RESULTS.

SO LET ME JUST SUM UP WHAT WE

FOUND.

SO I WANT TO EMPHASIZE AND I

THINK THIS IS IMPORTANT OF EVERY

STUDY THERE'S GOING TO BE
LIMITATIONS, CERTAINLY IN THIS
STUDY.
WE DO OUR BEST TO TRY MAKE IT
CAUSAL.
HOWEVER YOU CAN ALWAYS COME UP
WITH ALTERNATIVE EXPLANATIONS.
WE DON'T ACTUALLY SIT THERE IN
THAT PATIENT AND GENETIC
COUNSELING ROOM WHERE THEY GO
THROUGH PRIVACY, SPECULATING ON
THE MECHANISM, REVIEWING THE
PRIVACY POLICIES IN OTHER
STATES.
STUDY IN EARLY STATE OF
DIFFUSION SO THIS IS GOING TO BE
REPRESENTATIVE OF THE
INDIVIDUALS WHO EMBRACE NEW
TECHNOLOGIES EARLY.
HAVING SAID THAT, I THINK THERE
IS SOMETHING TO BE LEARNED WHICH
IS WHEN STATES GIVE MORE
CONTROL, OVER HOW PRIVATE

INFORMATION IS SHARED, WE DO SEE
AN INCREASE IN GENETIC TESTING.
AND WE SEE THIS INCREASE
PARTICULARLY FOR PEOPLE WHO ARE
WORRIED THERE MAY BE BAD NEWS
FROM THE GENETIC TEST.
NOW, WE FOUND THAT IN GENERAL,
INFORMED CONSENT, THAT IS GIVING
PEOPLE INFORMATION ABOUT HOW
THEIR DAY WILL BE USED BUT
WITHOUT GIVING THEM
CORRESPONDING CONTROL, JUST
DETERS PATIENTS AND BOTH
PATIENTS AND HOSPITALS FROM
HAVING GENETIC TESTS AND
OFFERING GENETIC TESTS.
LASTLY WE FIND THAT DATA USAGE
POLICIES HAVE ABSOLUTELY LITTLE
EFFECT, SO IT'S EITHER GOOD OR
BAD NEWS DEPENDING ON HOW YOU
LOOK AT IT.
I WAS QUITE POSITIVELY
ENCOURAGED BECAUSE USUALLY WHEN

I RUN A RELATIONSHIP, I FIND A
NEGATIVE EFFECT SO I WAS QUITE
PLEASED TO FIND NOTHING BAD.
ON THE OTHER HAND, THESE LAWS
ARE DESIGNED TO HELP PEOPLE AND
PERHAPS MY RESEARCH SUGGESTS
THAT THEY'RE ACTUALLY JUST NOT
BEING PUBLICIZED FLUFF TO
REASSURE PATIENTS.
SO WITH THAT I WILL SAY --
ENOUGH TO REASSURE PATIENTS.
WITH THAT I'LL SAY THANK YOU
VERY MUCH FOR ORGANIZATIONS
GIVING ME A CHANCE TO SPEAK.
[APPLAUSE]
>> THANK YOU, CATHERINE, NEXT UP
IS SASHA ROMANOSKY OF THE RAND
CORPORATION, INVESTIGATING THE
CAUSES AND COSTS OF
CYBER-INCIDENTS.
>> THIS HAS BEEN A LONG DAY,
ISN'T IT?
THANK YOU FOR FTC FOR HAVING US

HERE.

I'M SASHA ROMANOSKY.

I WILL PRESENT EMPIRICAL WORK

RELATED TO CYBER EVENTS, AYE

DEFINE THOSE IN A SECOND.

BUT I WANTED TO EXPLAIN A BIT OF

A MOTIVATION, TWO MOTIVATIONS

BEHIND THIS WORK, ONE IS YOU'VE

PROBABLY HEARD OF THIS EXECUTIVE

ORDER BY THE PRESIDENT A COUPLE

OF YEARS AGO TO HELP IMPROVE

CRITICAL INFRASTRUCTURE, AS PART

OF THAT NIS DEVELOPED THE

BEAUTIFUL FRAMEWORK FOR CYBER

SECURITY.

IF ANYONE HAS QUESTIONS ABOUT

HOW TO DEVELOP STANDARDS, IT

WILL TELL YOU EVERYTHING YOU

WANT TO KNOW.

THE TROUBLE WITH THAT -- THE

TROUBLE WITH THAT IS THAT IT'S A

VOLUNTARY STANDARD.

IT'S CERTAINLY NOT MEANT TO BE

REGULATED IN ANY KIND OF WAY, I
THINK DESPITE SOME OF THE
CRITICISMS THAT PEOPLE HAVE HAD.
AND SO THE QUESTION THEN
BECOMES, HOW DO YOU GET FIRMS TO
ADOPT?
HOW DO YOU GET FIRMS TO ADOPT
THESE STANDARDS?
WE THINK THEY'RE UNDERINVESTED
IN SECURITY SO HOW DO WE GET
THEM TO INCREASE THEIR SECURITY?
THAT'S A GREAT QUESTION.
SO THE STORY BEHIND THIS
EMPIRICAL WORK IS TRYING TO
UNDERSTAND THE INCENTIVES OR
FIRMS.
ARE THOSE INCENTIVES, DO THOSE
INCENTIVES EXIST TO ADOPT A
APPROPRIATE AMOUNT OF SECURITY
OR FAIR AMOUNT OF SECURITY OR
EFFICIENT AMOUNT OF SECURITY?
WE'RE GOING TO LOOK AT THAT.
THE OTHER MOTIVATION FOR ANYONE

WHO HAS HAD A CONVERSATION WITH
ME OVER THE PAST FEW YEARS KNOWS
I'M KEY ON CYBER INSURANCE.
THE KIND OF WORK THAT CYBER
INSURANCE CAN DO, UNDERSTANDING
THE VARIATION IN RISK ACROSS
FIRMS TO PRICE THAT AND THE KIND
OF DE FACTO POLICY THAT THEY ARE
CREATING NOW WITH THESE
POLICIES.
SO WITH THOSE, WITH THOSE
MOTIVATIONS WHAT I LOOK AT, THE
DATA SET I HAVE COMES FROM A
COMPANY CALLED ADVISANT.
TRADITIONALLY THEY LOOK AT LOSS
OF PROPERTY, OTHER KINDS OF
GENERAL LIABILITY, THAT FIRMS
WILL FACE.
THESE ARE CORPORATE DATA EVENTS
RELATED TO LOSS AND LITIGATION.
MOST OF THE DATA SETS THAT YOU
SEE OUT THERE RELATING TO CYBER
EVENTS INCLUDE 5,000, 6,000

OBSERVATIONS.

WE HAVE A DATA SET OF 12,000.

AS FAR AS I KNOW THIS IS THE

LARGEST DATA SET OF CYBER EVENTS

OF DATA BREACHES AND PRIVACY

VIOLATIONS, WHICH IS VERY NICE

WHICH ALLOWS US TO DO ANALYSIS

TO UNDERSTAND BETTER DIFFERENT

PATTERNS AND THE RISK THAT WE

WILL TALK ABOUT.

I'M SEPARATING THE DIFFERENT

KINDS OF EVENTS.

WHEN I SAY A CYBER EVENT THEY

ARE GENERALLY BROKEN INTO THESE

CATEGORIES AS I'M DEFINING THEM.

THERE ARE CERTAINLY OTHER WAYS

OF CATEGORIZING THEM FOR

PURPOSES OF MY TALK HERE.

I'M SEPARATING THEM INTO DATA

BREACHES.

WE NORMALLY TALK ABOUT AN

UNAUTHORIZED DISSEMINATION OF

PERSONAL INFORMATION, CAUSING

HARM TO A COMPANY, FOR EXAMPLE A
DENIAL OF SERVICE OR A THEFT OF
INTELLECTUAL INFORMATION,
UNAUTHORIZED USE OF PERSONAL
INFORMATION AND OTHER TYPES OF
PHISHING AND SKIMMING ATTACKS.
FOR THIS AUDIENCE WE'RE MORE
INTERESTED IN THE DATA BREACHES
AND THE PRIVACY INCIDENTS.
WHAT WE MIGHT THINK OF ACTS
CAUSED TO THE FIRMS, SO THEY ARE
BEARING, THEY ARE SUFFERING
THESE ATTACKS AS OPPOSED TO
PRIVACY VIOLATIONS WHERE THE
FIRM IS ENGAGING IN SOME KIND OF
ACTIVITY.
IT'S ALWAYS USEFUL TO UNDERSTAND
THE DATA JAILING PROCESS, TO
UNDERSTAND WHERE THE DATA ARE
COMING FROM AND WHAT'S INCLUDED
AND WHAT'S NOT INCLUDED.
SO TO BE CLEAR THESE DATA COME
FROM PUBLIC SOURCES.

THERE IS NO PROPRIETARY

INFORMATION.

ADVISANT, SCOURS LOCAL NEWS

SITES, USING THE FREEDOM OF

INFORMATION ACT, THEY USES

LEXLAW AND OTHER FIRMS.

EITHER BY THE FIRM BY A THIRD

PARTY BY CONSUMER BY LAW

ENFORCEMENT, SOMEHOW IT'S BEEN

OBSERVED BY THE FIRM.

WE OF COURSE HAVE NO INFORMATION

ABOUT THOSE EVENTS WHICH ARE NOT

DETECTED, NOT IN OUR DATA SET.

GIVEN DETECTION IT IS DISCLOSED

TO THE PUBLIC SO CERTAINLY OF

COURSE THERE IS NOT ALWAYS A

REQUIREMENT FOR A FIRM TO

DISCLOSE AN EVENT.

THERE ARE EXCEPTIONS EVEN WITH

THE BREACH NOTIFICATION LAWS SO

WE DO NOT OBSERVE THOSE THAT ARE

NOT BEING DISCLOSED.

CONDITIONAL ON DISCLOSURE, WE

WOULD HOPE WOULD BE REPORTED
WITHIN THIS DATA SET AND OF
THESE RECORDED IN THE DATA SET
WOULD LEAD TO ACTION, EITHER
CIVIL OR CRIMINAL.
TO GIVE YOU A SENSE OF THE
OVERALL TOTALS WE SEE THAT DATA
BREACHES HAVE BEEN IN FACT
INCREASING OVER THE PAST FEW
YEARS SO THESE CLAIMS BY OTHERS
THAT THERE ARE MORE BREACHES NOW
THAN THERE WERE BEFORE DO SEEM
TO BE TRUE.
HOWEVER WE FIND THAT THEY'RE
INCREASING AT A DECREASING RATE.
AS OPPOSED TO SECURITY INCIDENTS
PRIVACY VIOLATIONS AND THESE
PHISHING AND SKIMMING ATTACKS,
WHICH REPRESENT A MUCH SMALLER
PROPORTION OF THE OVERALL
INCIDENT.
SO WE SEE WE FIRST TAKE AWAY
FROM THIS IS THAT DATA BREACH

REALLY REPRESENTS A MAJORITY OF
THESE EVENTS.
SECURITY EVENTS SEEM TO BE
INCREASING AT AN INCREASING RATE
OVER THE PAST FEW YEARS.
AS FAR AS I KNOW, AN INCREASE IN
SECURITY INCIDENTS, CONDITIONAL
ON THE SAME LEVEL OF REPORTING,
WHAT THIS MIGHT SUGGEST IS FIRMS
MAY BE ATTACKED MORE NOW THAN
THEY WERE BEFORE.
IN RELATION TO THE -- IN REGARD
TO THE INSURANCE INDUSTRY AND
TRYING TO UNDERSTAND THE RISK OF
THEIR INSUREDS, ONE WAY IS TO
LOOK AT ANALYSIS BY INDUSTRY.
WHAT KINDS OF INDUSTRIES SUFFER
THE GREATEST NUMBER OF ATTACKS
OR POSE THE GREATEST RISK?
THERE ARE WAYS TO LOOK AT THIS,
WE COULD LOOK AT TOTAL NUMBER OF
EVENTS BY INDUSTRY BUT THAT
GIVES US AN INCOMPLETE PICTURE.

SO WE MIGHT LOOK AT THE INCIDENT RATE, THE PROPORTION OF FIRMS WITHIN A GIVEN INDUSTRY THAT SUFFER THE GREATEST NUMBER OF ATTACKS.

AND YOU COULD ALSO LOOK AT LAWSUITS AS AN AGGREGATE, COST OF EVENTS, I WON'T GO THROUGH ALL OF THESE IN THE INTEREST OF TIME.

BUT I'LL SHOW YOU THESE.

SO AS A FUNCTION OF TOTAL INCIDENTS, THE FINANCE AND INSURANCE INDUSTRY SUFFER THE GREATEST NUMBER OF INCIDENTS FOLLOWED BY HEALTH CARE AND GOVERNMENT.

EDUCATION AND THEN MANUFACTURING.

BUT IT'S A FUNCTION OF INCIDENT RATE, GOVERNMENT AGENCIES SO THESE ARE STATE AND LOCAL DMVs LAW ENFORCEMENT COURTS SUFFER

THE GREATEST INCIDENT RATE

FOLLOWED BY EDUCATION.

LET ME JUST SKIP THROUGH THESE.

AND THEN WE LOOK AT THE LEGAL

ACTIONS.

SO OF THE 1700 OR SO LEGAL

ACTIONS THAT WE HAVE RECORDED IN

THIS DATABASE, 300 OR SO ARE

CRIMINAL ACTIONS.

AND SOME FILED IN FEDERAL COURT,

SOME FILED IN STATE COURT.

BUT REALLY, THE BULK OF THESE

LEGAL ACTIONS ARE PRIVATE

ACTIONS BROUGHT -- PRIVATE CIVIL

ACTION BROUGHT IN FEDERAL CIVIL

COURT AND THESE WILL BE

ALLEGATION OF OF ALL KIND OF

COMMON LAW AND STATUTORY ISSUES.

UNJUST ENRICHMENT, A LITTLE

SMATTERING, FROM PREVIOUS

RESEARCH WE FOUND ALMOST 80

UNIQUE CAUSES OF ACTION BROUGHT

BY PLAINTIFFS IN THESE SUITS.

WHEN WE LOOK AT THE LITIGATION RATE, WE SEE THE PRIVACY LAWSUITS HAVE BEEN INCREASING DRAMATICALLY OVER THE YEARS WHEREAS THE DATA BREACHES HAVE BEEN HELD STEADY.

NOW THESE REPRESENT THE -- SPECIFICALLY THESE PRIVACY VIOLATIONS ARE -- IN REGARD TO THE LAWSUITS THE PRIVACY LAWSUITS, THE ALLEGATIONS REPRESENT CLAIMS OF TYPICALLY UNSOLICITED E-MAIL OR SPAM OR FAXING, UNSOLICITED TELEMARKETING, RECORDING, EITHER INDIVIDUAL GROW OR AUDIO RECORDING.

AN OVERALL THE LITIGATION RATE FOR DATA BREACHES AND SECURITY INCIDENTS HAVE BEEN DECREASING OVER THE YEARS WHICH CONFIRM SOME OF OUR PREVIOUS WORK, AND SO RIGHT NOW WE'RE LOOKING AT A

RATE OF ABOUT 3 OR 4%.

WHAT WE ALSO SHOW HERE IS THAT

YOU'LL NOTICE THAT THE

LITIGATION PRIVACY VIOLATIONS IS

REALLY QUITE HIGH, 95%.

I THINK THIS IS MORE OF AN

ARTIFACT OF THE DATA.

I THINK WHILE FOR DATA BREACHES

WE CAN UNDERSTAND THE SAMPLE OF

BREACHES AND IDENTIFY WHICH OF

THOSE HAVE BEEN LITIGATED

BECAUSE OF THE BREACH

NOTIFICATION LAWS BUT FOR

PRIVACY VIOLATIONS WE DON'T HAVE

THAT SAME DENOMINATOR.

WE DON'T UNDERSTAND THE TOTAL

NUMBER OF VIOLATIONS SO THE

PERCENTAGE THAT WOULD LEAD TO

LITIGATION.

IN OUR DATA SET ALL WE'RE

FINDING, WE'RE ONLY OBSERVING A

PRIVACY VIOLATION WHEN A LAWSUIT

IS OCCURRING.

NOW, THE NEXT QUESTION WE'RE
GOING TO LOOK AT SOME COST DATA
SO I WILL COUCH THIS BY SAYING
THAT THESE ARE ESTIMATES OF
COST, THEY DON'T INCLUDE --
CERTAINLY DON'T INCLUDE LOTS OF
OTHER INFORMATION.
THEY'RE ALL FIRM BASED, SO
TYPICALLY FIRST PARTY LOSSES AND
THIRD PARTY LOSSES.
ALL THE COST A FIRM WOULD OCCUR
BECAUSE OF A DATA BREACH THAT
YOU COULD IMAGINE.
THE COST OF NOTIFICATION, THE
COST OF FORENSICS, THE COST OF
REPAIRING ANY I.T. SYSTEMS.
IN SOME CASES THEY REPRESENT A
DOLLAR FIGURE LOSS, A FINANCIAL
LOSS.
THE THIRD PARTY LOSSES REPRESENT
THE COST OF LITIGATING, THE
LAWSUIT OF ANY KIND OF CONSUMER
REDRESS, OR FINANCIAL SANCTIONS

IMPOSED BY REGULATING AGENCIES.

SO GIVEN ALL THESE COSTS, THE

BIG QUESTION IS HOW MUCH DOES A

DATA BREACH COST?

SO PONEMAN AND OTHERS HAVE

PRODUCED SOME GREAT SURVEYS OVER

THE YEARS TRYING TO ESTIMATE

THESE COSTS AND WHAT THEY COME

UP WITH ARE TYPICALLY FIGURES OF

$5 MILLION, $7 MILLION AS THE

COST OF A DATA BREACH.

I MIGHT ARGUE THOUGH, THAT THIS

IS AN IMPROPER MEASURE BECAUSE

THEY ARE LOOKING AT THE MEAN,

THE STATISTICAL AVERAGE.

SO BECAUSE OF THE VARIATION OF

THE DISTRIBUTION OF THESE COSTS,

A MEDIAN IS A BETTER METRIC.

SO NOT EVERY DATA BREACH IS A

TARGET OF $270 MILLION AND

RISING.

NOT EVERY BREACH IS SONY, NOT

EVERY BREACH IS J.P. MORGAN OR

HOME DEPOT.

THERE ARE MANY AFFIRMS HAD DON'T

LOSE THAT MUCH MONEY.

WHAT WE FIND HERE IS MOST

COMPANIES LOSE LESS THAN

$200,000.

IF YOU WERE TO ASK ME THE

QUESTION OF HOW MUCH DOGS A DATA

BREACH COST I WOULD SAY LESS

THAN $200,000.

AND SO THIS IS GETTING BACK AT

THE INCENTIVES THAT FIRMS MAY OR

MAY NOT HAVE IN INVESTING IN

SECURITY AND PRIVACY PROTECTION

CONTROLS.

THE MEDIA COST IS A LITTLE BIT

HIGHER FOR PRIVACY VIOLATIONS, A

WORK WE'RE TRYING TO EXPLORE TO

UNDERSTAND EXACTLY WHY.

THE TAKE AWAY HERE IS THIS $5

MILLION, $7 MILLION COST IS

OVERBLOWN.

WE ALSO WANTED TO LOOK AT REPEAT

PLAYERS.

SO THIS NOTION COMES UP, QUITE A

BIT IN DIFFERENT CONVERSATIONS,

OF WHAT IS THE IMPACT TO FIRMS

THAT SUFFER MULTIPLE KINDS OF

EVENTS?

ARE THEY BEARING HIGHER

LITIGATION RATES, ARE THEY

BEARING HIGHER COST, HOW OFTEN

DO THEY OCCUR?

WE FINDER IN OUR DATA SET THAT

ALMOST 40% OF FIRMS ARE THESE

SO-CALLED REPEAT FIRMS, SUFFER

MULTIPLE EVENTS, THAT IS QUITE A

BIT HIGHER THAN I WOULD HAVE

THOUGHT BEFOREHAND.

I THINK THAT'S QUITE

EXTRAORDINARY IN FACT.

IN THE INFORMATION AND INSURANCE

SECTORS ALMOST 50% OF THEM ARE

REPEAT PLAYERS.

I THINK THAT IS QUITE

INTERESTING ALSO.

THE FIGURES HERE I'M SHOWING 9.5
MILLION VERSUS 4 ARE THE MEAN.
WHAT IT'S SHOWING YOU IS THE
COST FOR THESE REPEAT PLAYERS IS
ALMOST TWICE, A LITTLE OVER
TWICE THAN THE NON-REPEAT
PLAYERS, THOSE THAT SUFFER JUST
A SINGLE EVENT.
NOW THE MEDIANS ARE SHOWING
EXACTLY THE SAME THING THAT THE
COST IS HIGHER FOR THESE REPEAT
PLAYERS.
WHAT I THEN ALSO WANTED TO DO IS
TRY AND UNDERSTAND OKAY, MAYBE
200,000 IS ACTUALLY A LOT FOR
THESE FIRMS.
WHAT DOES THIS REPRESENT AS A
FUNCTION OF THEIR REVENUE?
WHAT I DID WAS WENT THROUGH ALL
OF THE DATA TO TRY AND
UNDERSTAND WHAT DO MOST
COMPANIES LOSE AS A FUNCTION OF
THEIR REVENUE AND THEN TRY AND

COUCH THAT RELATIVE TO DIFFERENT

KINDS OF LOSSES IN DIFFERENT

INDUSTRIES.

WE WANTED TO LOOK AT RETAIL,

HOSPITAL BAD DEBT GLOBAL PAYMENT

FRAUD.

WHAT YOU CAN IMAGINE IS VISA,

MASTERCARD HAVE A TOLERANCE FOR

BAD DEBT, THROUGH ORGANIC

PROCESS OR SOME CALCULATIONS

THEY HAVE SETTLED ON SOME

PERCENTAGE.

THESE NUMBERS COME FROM INDUSTRY

REPORTS.

SHOWING 5.9%, 5.2%, 3.1% FOR

FRAUD.

CYBER EVENTS, LESS THAN HALF A

PERCENT.

SO IT'S SAYING THAT CYBER EVENTS

COST LESS THAN HALF A PERCENT OF

A FIRM'S REVENUE, A GREAT DEAL

LESS THAN THESE OTHER -- THAN

THESE OTHER INDUSTRIES.

IN ADDITION TO THAT, IN OTHER WORKS, BY SOME COLLEAGUES, VILLY ABLON AT RAND, A GREAT SURVEY INSTRUMENT THE RAND HAS AVAILABLE TO IT TO TRY AND UNDERSTAND CONSUMER SENTIMENT TOWARDS BREACH NOTIFICATION.

HOW DO THEY FEEL IN RESPONSE TO FIRMS GETTING THESE NOTICES OF A DATA BREACH?

WHAT WE FIND IS THAT FOR THE MOST PART THEY'RE REALLY QUITE CONTENT.

THEY ARE QUITE HAPPY WITH THE TIMELINESS, INFORMATION PRESENTED IN THE NOTIFICATIONS, AND REALLY HAVE GENERALLY NO CONCERNS.

THERE WAS A SMALL PERCENTAGE OF THEM THAT MAY CHANGE FIRMS BUT BY AND LARGE THEY ARE REALLY QUITE HAPPY.

SO CONSUMER SENTIMENT IF IT IS

IN FACT HIGH COUPLED WITH A

SMALL COST TO A FIRM BECAUSE OF

THESE EVENTS, REALLY MAY SUGGEST

THAT FIRMS HAVE VERY LITTLE

INCENTIVE TO CHANGE THEIR

PRACTICES.

THANK YOU VERY MUCH.

[APPLAUSE]

>> THERE IT IS.

THANK YOU SASHA AND THANK YOU TO

EVERYONE FOR THOSE

PRESENTATIONS.

THEY WERE WONDERFUL.

AND VERY VARIED, SO I WANT TO

RECAP THEM BRIEFLY BUT FIRST I

WANT TO INTRODUCE DOUG SMITH WHO

IS FROM THE FEDERAL TRADE

COMMISSION AND SIONA LISTOKIN.

WE HAD FOUR DIFFERENT

PRESENTATIONS, JENS PRESENTED

BUG BOUNTY AND VERONICA AND

ALESSANDRO PROPOSED AN ECONOMIC

MODEL FOR ADVERTISERS, PLATFORMS

AND CONSUMERS AND CONCLUDED THAT
THE ALLOCATIONS OF SHARING
CONSUMER INFORMATION TENDS TO
BENEFIT THE PLATFORM AND THE
ADVERTISER.
IF I'M WRONG YOU CAN TELL ME IN
JUST A SECOND.
CATHERINE PRESENTED A STUDY OF
THE RATE OF CONCLUDED THAT
STATES WHERE REDISCLOSURES
RESTRICTED HAVE THE HIGHEST
TESTING RATES AND THAT STATES
WITH INFORMED CONSENT DECREASES
THE RATE OF GENETIC TESTING.
AND FINALLY SASHA LOOKED AT ONE
SET OF DATA, AND OFFERED
CONCLUSIONS ABOUT THE MEDIAN
COST OF CYBER EVENTS PUTTING IT
AROUND 200,000 AND LESS ATHAN
WHAT OTHER STUDIES HAVE FOUND
ABOUT THE COST OF CYBER EVENTS.
TO START I OFF I WANT TO TURN IT
OVER TO SIONA.

>> KEVIN HAD ASKED ME TO TALK
ABOUT THEMES IN THIS PANEL AND I
WOULD NOTE THAT THE TITLE OF THE
PANEL IS THE ECONOMICS OF
PRIVACY AND SECURITY AND I THINK
THAT'S ABOUT AS CLOSE AS WE'LL
GET TO A THEME.
LOTS OF VARIATION HERE.
PAPERS COVERED SOME OF THE MOST
IMPORTANT OR TOUCHSTONE TOPICS
IN PRIVACY, HEALTH DATA, ONLINE
ADVERTISING AND OF COURSE
SECURITY.
ALSO POINT OUT THAT THE PANEL
HAD A LOT MORE FOCUS ON HOW
FIRMS RESPOND TO INCENTIVES AND
NOT JUST CONSUMERS.
AND FINALLY, A LOT OF TALK OR
THE PAPERS HERE REALLY ARE A
CROSS-SECTION OF STAGES OF
RESEARCH DESIGN.
SO IF YOU THINK ABOUT ECONOMICS
OF PRIVACY YOU HAVE A MODEL THAT

EXTENDS EXISTING THEORY, NEW
DATA SETS AND EXPLANATORY OR
CAUSAL PAPERS.
SO MY METATHEME HER IS THAT THE
FIELD OF ECONOMICS OF PRIVACY IS
ALIVE AND WELL AND QUITE ROBUST
BUT THAT'S GOING TO BE MY
QUESTION.
SO EXTENDING COMMISSIONER
BRILL'S COMMENTS AFTER LUNCH AND
THE CONCLUSION AT THE END OF
VERONICA AND ALESSANDRO'S PAPER,
IN THIS FIELD WHERE WHAT'S YOUR
WISH LIST?
THIS IS FOR EVERYONE.
WHERE DO YOU SEE THE GAPS IN
THIS LITERATURE?
SPECIFICALLY AS IT WOULD RELATE
TO POLICY MAKERS AND INDUSTRY
PRACTICE.
SO NOT JUST ADVANCING ACADEMIC
RESEARCH.
I'LL START WITH VERONICA AND

ALESSANDRO BUT I'M INTERESTED IN
EVERYONE'S THOUGHTS.
>> ONE COMMENT AND I'LL
PIGGYBACK ON OUR LAST SLIDES
ABOUT THE PIECE IN JAIL WHICH A
LOT OF SSRN.
IN DOING THAT REVIEW OF THE
LITERATURE OF ECONOMICS OF
PRIVACY WE IDENTIFIED THREE
WAVES OF RESEARCH.
THE FIELD IS NOT NOVEL AT ALL.
IT STARTED IN THE LATE 1970s,
EARLY 1980s.
THERE IS A SCHOOL OF SCHOLARS,
THERE IS A BEAUTIFUL PEDIGREE
AND ALSO QUITE A BIT OF WORK
STARTING BACK 40 YEARS OR SO.
HOWEVER, ONLY IN THE TIME THERE
WERE NO MODELS, BACK IN LATE
'70s EARLY 80s, NO MODELS OR
MICROECONOMICS IN THE FIELD OF
PRIVACY WAS MORE ABOUT USING
ECONOMIC CONCEPTS SUCH AS

SYMMETRIC INFORMATION, APPLIED

TO PRIVACY.

WHAT WE HAVE NOW IS LOTS OF

CAREFULLY MODEL -- CAREFUL

MODELING WORK.

THANKS TO THE WORK OF THINGS

LIKE CATHERINE TUCKER AND OTHERS

IT'S BEAUTIFUL EMPIRICAL WORKS.

IN TERMS OF MY WISH LIST IS TO

SEE MORE EMPIRICAL WORK AND IN

ORDER TO HAVE MORE EMPIRICAL

WORK, SOMETIMES WE NEAT DATA

FROM THE INDUSTRY.

IF THE INDUSTRY IS SERIOUS AND

SEES THE DATA AS MORE OIL, GOOD

FOR EVERYONE THEN WE SHOULD HAVE

ADDRESSED THE PROBLEM OF

INFORMATION SYMMETRY THAT SURGE

WAS REFERRING TO AS ONE OF THE

CRUCIAL PROBLEMS WE HAVE IN THE

PREVIOUS PANEL, WE WANT MORE

DATA FROM THE INDUSTRY REGARDING

EXACTLY WHAT THEY DO FROM THE

INFORMATION THEY COLLECT.

MAY NOT CARE ABOUT WHAT

COMPANIES ARE DOING.

RESEARCHERS CAN ACTUALLY STUDY

THE DATA AND THEN COME OUT

AGGREGATIVE, AND COME UP WITH

POLICY RECOMMENDATION.

SO MY WISH LIST IS MORE

EMPIRICAL WORK AND MORE

TRANSPARENCY FROM THE INDUSTRY

SIDE.

>> I MEAN I WOULD ECHO THAT,

RIGHT?

I THINK THERE'S BEEN A LOT OF

TIME SPENT DOING WHAT A

COLLEAGUE WOULD REFER TO AS

ADMIRING THE PROBLEM.

AND I THINK THAT'S USEFUL,

THAT'S GOOD, I THINK THAT ONLY

GETS US SO FAR.

I LIKE EMPIRICAL WORK BECAUSE IT

SPEAKS TO EVIDENCE FOR

SOMETHING.

IT GETS US PAST NORMATIVES, AND
HELPS US ANSWER THE HE EFFECT,
WHAT THE EFFECT WILL BE A ON B,
THE GOLD STANDARD, IN ORDER TO
DO THAT, THE POINT IS EXACTLY
TRUE.
YOU KNOW, WE NEED DATA, RIGHT?
AND SOMETIMES, THAT TAKES US
BEING VERY CREATIVE ON FINDING
IT IN CLEVER WAYS LIKE THE
PREVIOUS PANEL, THE RESEARCHERS
DID THEMSELVES, COMING UP WITH
THESE SPEERMTS WHICH I THINK
ISs -- EXPERIMENTS, WHICH
TAKES PAIN, THAT IS OKAY TOO,
BUT I WOULD ECHO EVERYTHING
ALESSANDRO HAD TO SAY,
ESPECIALLY IN THE WONDERFUL
ACCENTED WAY THAT HE SAID IT.
>> WELL I WOULD ADD TO THE
ACCENTS.
SO I -- YOU KNOW UNSURPRISINGLY
I AGREE FOR THE NEED FOR

EMPIRICAL WORK.

WHAT ALWAYS STRIKES ME IS IF I'M

A POLICY MAKER TRYING TO DECIDE

IF I WANT THE MINIMUM WAGE, WHAT

LEVEL THE MINIMUM WAGE SHOULD

BE, I COULD DRAW ON HUNDREDS OF

ECONOMIC STUDIES THAT HAVE

MEASURED AND HAVE HUNDREDS OF

DIFFERENT WAYS HOW MINIMUM WAGES

AFFECT WAGE LEVELS.

HOWEVER IF I'M A POLICY MAKER

MAKING REALLY IMPORTANT

DECISIONS ABOUT WHETHER TO

RELATING PRIVACY OR DATA, I'M

INSTEAD RELYING ON JUST A

HANDFUL OF STUDIES IN

POTENTIALLY NONGENERALIZABLE

SPHERES.

ITS PERSONNEL AND NUMEROSITY.

>> THE LOSS OF PRIVACY AND SOME

WORK THAT ALESSANDRO AND I HAVE

DONE GOES IN THAT DIRECTION TO

UNDERSTAND HOW PEOPLE PERCEIVE

POLICY MAKING OVER TIME BUT WHAT
WE COULD NOT ASSESS IN A ROBUST
MANNER IS WHAT ARE ACTUALLY THE
POTENTIAL LOSSES THAT WE MAY
FACE DOWN THE ROAD.
AND I THINK THIS IS A VERY
CRITICAL ISSUE WHEN IT COMES TO
GENETIC PRIVACY BUT ALSO TO
CONSUMER PRIVACY.
A SIMILAR ISSUE ALSO RISES WHERE
THE TO SECURITY, WHERE ACTUALLY
THINGS MIGHT ARISE IN THE
CONTEXT OF WHAT WE DO NOT
OBSERVE.
YOU SAW IT IN SASHA'S CHART.
WE COULD ONLY ANALYZE THE DATA
THAT WAS DETECTED.
SO WHAT ABOUT ALL THE SECURITY
BREACHES THAT WE DO NOT OBSERVE
AND WE KNOW NOTHING ABOUT?
SIMILAR WITH RESPECT TO MY
PRESENTATION, WHEREAS THE
BEHAVIOR OF WHITEHATS, WE WE CAN

OBSERVE, WHAT WE DO NOT OBSERVE
IS THE BEHAVIOR OF BLACKHATS AND
THERE WE STILL HAVE A LOT OF
WORK TO BE DONE IN TERMS OF
INVESTIGATING THEM AND GETTING
MAYBE QUALITATIVE DATA BUT ALSO
TYING TOGETHER DATA SETS SUCH AS
SASHA'S WITH ANALYSIS THAT WE
HAVE DONE, TO KIND OF BE ABLE TO
INFER WHERE VULNERABILITIES HAVE
BEEN KNOWN THAT HAVE NOT BEEN
DISCOVERED BY THE WHITEHATS.
>> SOMETHING REALLY IMPORTANT
ABOUT LONG TERM EFFECTS AND HERE
IS THE DILEMMA, THE DILEMMA THAT
THE FIELD THE ECONOMICS OF
PRIVACY FACES.
IN MY RUE, THE EFFECT IS LONG
TERM, ECONOMIES THAT WE CAN
PUBLISH AND DO RIGOROUS WORK, IT
IS VERY, VERY DIFFICULT TO DO
STUDIES AND FOUND CAUSAL LINKS
OVER, WHEN THERE COULD BE A DATA

BREACH NOW WHICH IS ONLY IN
EFFECT SEVEN YEARS LATER.
AND YOU ARE NOT GOING TO SATISFY
REVIEWERS IN LEGAL HISTORIC
JOURNAL TO FIND THESE KINDS OF
EFFECTS.
I DON'T THINK THERE IS ANY
SIMPLE METHODOLOGICAL EFFECTS.
>> CATHERINE, YOUR RESEARCH
SHOWED EFFECTS ON CONSUMERS
CHOICES IN THE CONTEXT OF
GENETIC PRIVACY.
I WAS CURIOUS JUST HOW YOU THINK
THIS RESEARCH, WHAT IMPLICATIONS
IT HAS FOR OTHER AREAS OF
PRIVACY?
>> OKAY, SO WHAT WAS NICE ABOUT
THIS SETTING IS IT ALLOWED US TO
HAVE MORE OF A HORSERACE WHERE
WE HAD THE SAME THING WE WERE
TRYING TO EXPLAIN IN LOTS OF
DIFFERENT PRIVACY REGIMES.
NOW, THE EXTENT OF -- THE REASON

I FIND IT USEFUL OR REASSURING
IS IT HELPS ME BELIEVE SOME OF
THE RESEARCH I'VE DONE IN OTHER
AREAS WHICH HAVE BEEN MORE
CASE-BY-CASE.
ON THE RESEARCH I'VE DONE FOR
EXAMPLE IN TARGETED ADVERTISING
WHICH A LOT OF PEOPLE HAVE
TALKED ABOUT TODAY HAS
EMPHASIZED THE NEGATIVE EFFECTS
OF INFORMED CONSENT BUT ALSO
POSITIVE EFFECTS FROM IMPROVE BE
CONSUMER PERCEPTIONS OF CONTROL.
I WAS ALWAYS NERVOUS BECAUSE
THOSE WERE TWO VERY SEPARATE
STUDIES, DIFFERENT TIMES
DIFFERENT STUDIES EVEN DIFFERENT
COUNTRIES.
I FOUND IT REASSURING TO USE
THIS HORSERACE, TO MAKE ME THINK
PERHAPS THERE IS SOMETHING MORE
GENERALIZABLE TO STUDY THE
EFFECTS OF DIFFERENT PRIVACY

REGIMES.

>> THANKS.

THE QUESTION I HAVE FOR THE

GROUP IS ACTUALLY A LITTLE BIT

OF A FOLLOW-UP ON ONE OF THE

THINGS SIONA POINTED OUT WHICH

IS, YOU GUYS ARE LOOKING A LOT

AT HOW FIRMS' CHOICES ARE HAVING

IN THIS ARENA.

SO WHAT ARE THESE PAPERS AND

RESEARCH IN GENERAL SUGGEST

ABOUT WHAT THE PRIVATE SECTOR IS

GETTING RIGHT, WHAT IT'S GETTING

WRONG?

YOU KNOW WHAT CAN THIS IMPROVE

ON OUR UNDERSTANDING OF WHAT

KIND OF MARKET FAILURES WE MIGHT

BE CONCERNED ABOUT IN THIS AREA?

WHY DON'T WE START AT THIS END I

GUESS?

>> I THINK ONE OBSERVATION THAT

ALESSANDRO AND I HAVE MADE OVER

TIME, WE HAVE SOONER A LOT OF

PRIVATE ENTITIES ENTERING THE
MARKET WITH PRIVACY ENHANCING
OFFERS BUT NOT PICKED UP IN THE
MARKETPLACE IN A SUFFICIENT
DEGREE.
SO WELL, THE GOOD NEWS IS THAT
WE DO SEE THESE OFFERS, WE SEE A
LOT OF TECHNOLOGICAL SOLUTIONS
THAT ARE EVENTUALLY PICKED UP BY
STARTUPS.
BUT WHAT WE SEE LESS IS AN
ADOPTION BY THE BIG PLAYERS,
BECAUSE OF A LACK OF INCENTIVES.
TARGETING MARKETING IS JUST TOO
ENTICING TO GIVE IT UP IN
EXCHANGE FOR MORE PRIVACY
FRIENDLY PRACTICAL SOLUTION.
SO THERE'S A FUNDAMENTAL
CONUNDRUM THAT WE ARE PRESENTED
WITH THAT IS VERY HARD TO SIDE
STEP.
NEVERTHELESS I THINK IT'S VERY
IMPORTANT THAT WE SEE THESE NEW

OFFERS IN THE MARKETPLACE AND I
HOPE MORE OF THEM ARE ACTUALLY
PICKED UP IN PRACTICE.
>> WHAT ARE THEY GETTING RIGHT?
>> ONE REASON FOR OPTIMISM IS
THE SENSE OF PRIVACY, ANNOUNCING
TECHNOLOGIES, ALMOST EVERY TIME
OF YEAR, TALKING ABOUT PATs
BECAUSE I STRONGLY THINK THAT
TECHNOLOGY, CAN BE A SOLUTION,
TECHNOLOGIES DO NOT STOP
ALTOGETHER THE FLOW OF DATA BUT
RATHER MODULATE THE SHARING OF
PROTECTION.
PRIEIVES FIRMS CAN ACTUALLY
MAKE, THIS MAY BE WISHFUL
THINKING BUT MAY BE PROACTIVITY
IN DEPLOYING P.A.T.S, SO THEY
CAN STILL DO MUCH OF WHAT THEY
ARE DOING NOW BUT IN A MORE
PRIVACY PRESERVING MATTER.
NOW TRUTH TO BE TOLD, SOME OF
THESE TECHNOLOGIES ARE STILL IN

THEIR INFANCY.

FOR INSTANCE AAMORPHIC

ENCRYPTION, PROMISING FOR MOMENT

AND I DO BELIEVE THAT WE COULD

IN THE SPACE OF PRIVACY WE CAN

ACTUALLY HAVE THE CAKE AND EAT

IT TOO BECAUSE OF THESE

TECHNOLOGIES.

>> IN TERMS OF WHAT ARE FIRMS

GETTING RIGHT, GOD, THAT'S SUCH

A GOOD QUESTION AND I WISH I HAD

A BETTER ANSWER THAN THE ONE I'M

ABOUT TO GIVE.

I THINK -- SO I THINK WHAT WE

CAN RELY ON IS THAT FIRMS

WILL -- FIRMS WILL OPERATE BASED

ON INCENTIVES.

AND THE GOAL THEN IS TO TWEAK

THE INCENTIVES SUCH THAT THEY

BECOME ALIGNED FOR ALL THE

PLAYERS, RIGHT?

THAT'S NOT NEW.

AND WHAT THAT MEANS IS THAT, YOU

KNOW, LOOK IF PRIVACY REALLY IS

A BIG DEAL THEN CONSUMERS SHOULD

REALLY ACT LIKE IT'S A BIG DEAL.

AND IF AND ONLY UNTIL THEY DO

WILL FIRMS HAVE INCENTIVE TO

TAKE IT SERIOUSLY.

SO I GUESS I NEED -- I GUESS I

WOULD SAY THAT CONSUMERS SHOULD

TAKE IT SERIOUSLY, AND ACT LIKE

IT, AND THEN FIRMS WILL TAKE IT

SEERLZ.

NOW IF THERE ARE -- SEECIALS.

SERIOUSLY.

IF THERE ARE MARKET FAILURES FOR

WHICH FIRMS CAN'T IMPOSE ANY

KIND OF EFFECT ON THE FIRM THEN

THAT'S WHERE REGULATION OR

POLICY OR FTC ACTIONS CAN COME

INTO PLAY.

GO AHEAD.

>> NO, I JUST WANTED TO BUILD

OPEN THAT.

BECAUSE I THINK -- I THINK WHAT

I OFTEN SEE IN THE DISCUSSION IS
THIS UNDERLYING ASSUMPTION THAT
IT'S NEVER IN FIRMS' INTEREST TO
REGULATE ON PRIVACY.
AND THEREFORE, GOVERNMENT HAS TO
INTERVENE.
BUT I THINK THERE ARE INSTANCES
THAT WE SEE IN RESEARCH WHERE
THERE ARE INCENTIVES FOR FIRMS
TO ACTUALLY IMPROVE PRIVACY
PROTECTIONS FOR CONSUMERS.
FOR EXAMPLE, THE PROVISION OF
USER CENTRIC CONTROLS.
AND SO I SORT OF SEE THAT AS A
BEAM OF LIGHT IN AN ALSO CYNICAL
WORLD.
>> I THINK IT DOES TOUCH ON THE
WORLD OF INFORMATION DISCLOSURE
AND CHOICE AND NOTICE.
AND POOR CHOICE AND NOTICE.
YOU KNOW, POOR CHOICE, OVER THE
PAST FIVE, SIX YEARS HAS TAKEN A
BEATING, HASN'T IT?

BUT IT'S RELIED ON THE NOTION
THAT FIRMS DON'T BEHAVE THE
RIGHT WAY, CONSUMERS DON'T
BEHAVE THE RIGHT WAY BECAUSE
THEY DON'T HAVE THE RIGHT
INFORMATION.
ONLY IF WE COULD GIVE THEM THE
RIGHT INFORMATION WOULD THEY
MAKE THE PROPER CHOICES?
AH, I'M JUST NOT SURE THAT'S
TRUE.
AT LEAST LET ME SAY IT THIS WAY.
THAT MAYBE FIRMS AT LEAST IN MY
CASE WITH THE DATA, THAT MAYBE
FIRMS DO HAVE THE RIGHT
INFORMATION.
MAYBE THEY ARE AWARE OF ALL THE
RISKS THAT USING AND COLLECTING
THE DATA HAVE AND MAYBE THEY ARE
MAKING RATIONAL CHOICES AND FOR
THEM INVESTING A CERTAIN AMOUNT
WHICH WE MAY THINK IS
UNDERINVESTING ISN'T THE PROPER

AMOUNT.

BUT MAYBE IT IS ACTUALLY THE

RIGHT AMOUNT AS FAR AS THEY'RE

CONCERNED.

>> I JUST WANT TO ALSO ADD THAT

THIS PANEL WAS ALSO ABOUT

SECURITY.

AND I THINK ONE THING THAT FIRMS

DO RIGHT IS PARTICIPATING IN

BUCK BUOYANT -- BUCK BOUNTY

PROGRAMS.

HEIGHTENING WEB SECURITY AND

OTHER SECURITY ASPECTS.

I THINK THEY'RE STILL QUITE A

STEP AWAY FROM ANYTHING

APPROACHING FULL SECURITY.

BUT I THINK HAVING A

MULTIDIMENSIONAL SECURITY

PROGRAM INCLUDING BUCK BOUNTY

PROGRAMS ARE A CORRECT

DIRECTION.

>> JENS, I WANTED TO ASK YOU,

THERE WAS A NOTORIOUS BLOG POST

ON THE CHIEF INFORMATION OFFICER
OF ORACLE, BEHAVIORAL THE
ANALYSIS WAS IT'S VERY EXPENSIVE
TO GO THROUGH THESE BUG REPORTS,
IT VERY RARELY YIELDS USEFUL
INFORMATION.
YOUR STUDY SHOWS THERE ARE
BENEFITS TO PARTICIPATION BUT
THE QUESTION SHE WAS RAISING IS,
ARE THE BENEFITS OF
PARTICIPATION GREATER THAN USING
THAT SAME MONEY TO PAY ANOTHER
ENGINEER TO EVALUATE INTERNALLY
THE CONTROLS ON YOUR SOFTWARE?
>> SO BUCK BOUNTY PROGRAMS ARE
NOT THE FIRST SECURITY MEASURE
THAT ANY COMPANY SHOULD
IMPLEMENT.
HOWEVER AS YOU SAW IN ONE OF MY
EARLY SLIDES VERY MATURE
COMPANIES, RUNNING THEIR OWN
BUCK BOUNTY PROGRAMS LIKE
FACEBOOK, GOOGLE AND SO ON.

SO FROM THAT PERSPECTIVE IT WAS
WORTH THEIR WHILE.
SO CERTAINLY ONE OF THE MAIN
SELLING POINTS IS IT PROVIDES A
DIFFERENT PERSPECTIVE, IN
ADDITION TO RUNNING SOFTWARE
SECURITY TOOLS, HAVE SECURITY
RESEARCHERS IN THE SENSE THAT
WHITEHAT RESEARCHERS HAVE
SOMEWHAT MORE OF A VIEW LIKE A
BLACKHATTED ORGANIZATION, THEY
ARE MORE CREATIVE, IN PLACES
WHERE OTHER SECURITY RESEARCHERS
WOULD NOT LOOK, A GOOD SECURITY
POINT TO INCH THE SECURITY OF
YOUR WEBSITE EVEN A COUPLE OF
STEPS FURTHER.
THERE IS ALSO A LOT OF CRITICISM
ABOUT THESE BAD RATIOS, THE DATA
THAT IS ACTUALLY THEN USEFUL AND
I THINK WHEN YOU ACTUALLY LOOK
VERY CLOSELY AT THAT A LOT HAS
TO DO WITH THE MATTER OF

DUPLICATE REPORTS.

I MEAN THIS IS WHEAL WHITEHAT

RESEARCH DOING THEIR JOB.

IF RESEARCH HASN'T BEEN THIS

CLOSE THEY WILL REPORT

OFTENTIMES THE SAME KIND OF

SECURITY WEAKNESSES TO THE

PARTICULAR ENTITIES, AND WELL,

TAKING THIS INTO ACCOUNT AND

ACTUALLY THE ERROR RATE IS NOT

THAT HIGH.

LAST POINT HERE IS THAT HERE,

ACTUALLY, THE INVOLVEMENTS OF

BUCK BOUNTY PROGRAMS, CAN

INTRODUCE MEASURES SUCH AS

REPUTATION MECHANISMS,

COORDINATE REWARDS AND SO ON

THAT ACTUALLY THEN ALSO INSTILL

SOME PART OF COMPETITION,

BETWEEN THE WHITEHAT COMMUNITY

PARTICIPANTS SO THAT THEY ARE

MORE INCLINED TO ACTUALLY

PROVIDE HIGH QUALITY DATA TO THE

PARTICIPATING COMPANIES.

>> ALL RIGHT, WE HAVE 20 SECONDS

LEFT.

SO SIONA DO YOU HAVE ANY FINAL

THOUGHTS?

>> CAN I JUST CLARIFY SOMETHING?

>> VERONICA, PLEASE.

>> I WANTED TO CLARIFY IN OUR

FINDINGS WE DON'T FIND AN

INTERMEDIARY IS ALWAYS BAD BUT

SOMETIMES THEY DO THE RIGHT

THINGS FOR CONSUMERS.

SO THERE ARE POLICIES IN THEE

CASES MORE THAN ONCE.

THERE ARE CASES IN WHICH THE

INTERESTED INTERMEDIARY IS

ALIGNED WITH THE CONSUMERS, BUT

MAY BE CONTRASTING WITH THE

CONSUMERS.

>> YOUR PAPER ISN'T CURRENTLY ON

OUR WEBSITE BUT I BELIEVE WE

WILL HAVE IT UP FOLLOWING THIS

PRESENTATION SO IF PEOPLE WANT

MORE INFORMATION ABOUT YOUR

FINDINGS THEY CAN LOOK AT IT

THERE.

THANK YOU ALL FOR PARTICIPATING

IN THIS SESSION, WE REALLY

APPRECIATE IT, THANK YOU.

[APPLAUSE]