

The Big Picture: Comprehensive Online Data Collection
Transcript
December 6, 2012
12:00 PM

Session 2

>> I THINK WE'RE GOING TO GET STARTED.
GOOD MORNING AND WELCOME TO OUR FIRST PANEL OF THE DAY.
THIS PANEL WILL FOCUS ON THE DATA COLLECTION LANDSCAPE AND BENEFITS AND RISKS OF COMPREHENSIVE DATA COLLECTION AS WE'RE DEFINING AS THE COLLECTION OF DATA OF ALL OR MOST OF CONSUMERS ON-LINE ACTIVITIES ACROSS MULTIPLE ACTIVITIES OUR PANELISTS INCLUDE MIKE ALTSCHUL, PROFESSOR KNEEL RICHARD FROM WASHINGTON UNIVERSITY IN ST. LOUIS, ASHKAN AS WELL SOLTANI A TECHNOLOGIST, INDEPENDENT RESEARCHER AND CONSULTANT. NEXT TO HIM WE HAVE PROFESSOR HOWARD BEALS, THEN MARKHAM ERICKSON FOR THE INTER KNELT ASSOCIATION --D NO AUDIO.
>> -- CARE ABOUT THE SELECTION SO MUCH ST-Z AVAILABLE TO EVERYONE.
OFTEN TIMES IT'S THE CONTENT OF THE COMMUNICATION.
THIS IS THE CONTENT OF E-MAIL COUNCIL LOADED OR CONTENT OF INFORMATION I POST TO A WEBSITE OR THE METADATA ASSOCIATED WITH THE WEB OR MOBILE DEVICES SUCH AS LOCATION INFORMATION. BROWSING HISTORY.
THIS TYPE OF STUFF I THINK IS OF CONCERN.
ON ONE HAND THE ISSUE OF HOW MUCH OF -- OF THE INFORMATION IS

COLLECTED, YOU KNOW, IN TERMS IS ALL OF THE INFORMATION AND META INFORMATION.

THE OTHER CONCERN IS THE COVERAGE OF THE AMOUNT OF INFORMATION COLLECTED.

SOME OF MY RESEARCH IN THE PAST SHOWS SINGULAR ENTITIES.

ONE ENTITY CAN CAPTURE UP TO 88% OF THE INFORMATION THEY WOULD FIND JUST RIGHT, FIND

>> THE PAPER JUST PUBLISHED.

>> -- IDENTIFY DRUG INTERACTIONS BETWEEN DRUGS PUT INTO SEARCH ENGINES AND QUERIED ARE FAR MORE EFFECTIVE FOR IDENTIFYING THOSE PROBLEMS.

SO MAKING INFORMATION VISIBLE IS CERTAINLY ONE BENEFIT.

OF COURSE MORE ACCURATE PERFORMANCE INFORMATION.

AS HAN MENTIONED ADVERTISING METRICS MAKING SURE THAT MONEY IS BEING SPENT IN THE MOST EFFECTIVE WAY TO REACH TARGETED AUDIENCES OR CONSUMERS.

MORE ABOUT PRODUCT SUPPORT TEST

PROVIDING FREE ADVERTISER SUPPORTS

HELLO?

>>

>> A HOW THEY'RE USED.

AND I HAVE, MY OBSERVATION HAS BEEN THAT, THAT FREEING UP DATA AND HAVING MORE DATA IS GOOD.

IT ALLOWS US TO MAKE BETTER DECISIONS.

DATA DRIVEN DECISIONS.

THINGS THAT HAVEN'T SURFACED IN THE PAST.

GOVERNMENT INFORMATION IS MADE AVAILABLE.

THAT, THAT IS FAR BETTER THAN THE REVERSE WHICH IS LOCKING UP DATA, AND -- AND HAVING DATA NOT AS ACCESSIBLE.

SO, I THINK WHEN WE TALK ABOUT COMPREHENSIVE DATA COLLECTION WE NEED TO TALK ABOUT THE USES OF THE DATA COLLECTION.

IN TERMS OF WHAT TYPES OF DATA ARE VALUABLE TO INTERNET COMPANIES IT REALLY DEPENDS ON THE TYPES OF SERVICES WE'RE TALKING ABOUT.

FOR EVERY DIFFERENT SERVICE THE DATA THEY NEED TO PROVIDE THEIR SERVICES IS GOING TO BE, IS GOING TO BE WILDLY DIFFERENT.

>> I WOULD LIKE TO JUMP IN FOR A SECOND.

SO, YA THERE ARE GOING TO BE POTENTIAL BENEFITS FOR THIS BIG DATA.

I THINK IT'S REALLY IMPORTANT TO, TO KEEP IN MIND THAT ONE OF THE PREMISES OF THIS IS WHAT I CREDIT A IN SEEDIOUS ETHICAL PREMISE.

WHICH IS THAT COLLECTING DATA ABOUT PEOPLE, FROM PEOPLE, WITHOUT THEIR KNOWLEDGE OR UNDERSTANDING OF WHAT ASK BEING COLLECTED OR WHO IS COLLECTING IT IS FUNDAMENTALLY DIFFERENT FROM SAY TAKING TEMPERATURE READINGS OF THE, YOU KNOW, EARTH'S CRUST OR SOMETHING LIKE THAT.

THE TARGET EXAMPLE WHICH EVERYONE KNOWS WHICH DAN MENTIONS THIS MORNING IS A REALLY NICE EXAMPLE OF HOW -- WHAT SEEM LIKE INNOCENT FACTS. YOUR PURCHASES OF SRAOEUT MY SUPPLEMENTS AND LOTIONS, AND UNSCENTED TISSUES TO NAME I THINK THROW OUT OF 25 COMPONENTS.

PREGNANCY PREDICTIONS.

WE'RE ABLE TO ALLOW SOMEONE THAT REALLY SHOULDN'T KNOW WHETHER

YOU'RE PREGNANT TO ACTUALLY
FIGURE THAT OUT WITH A
TREMENDOUS ACCURACY.
THIS IS A SITUATION WHERE THE
PERSON -- THIS ISN'T A SITUATION
WHERE THE PERSON VOLUNTEERED
THAT OR BOUGHT A PRODUCT ABOUT
IT.

IT'S BECAUSE WE HAVE SO MUCH
DATA.

BECAUSE SOME PEOPLE VOLUNTEERED
DATA ABOUT THEIR PREGNANCY
STATUS AS PART OF TARGET'S BABY
SHOWER REGISTRY.

THEN COMBINE WITH ALL OF OUR,
ALL OF THE OTHER DATA YOU ARE
ABLE TO MAKE HIGH POGT SEES AND
TEST THEM ON ALL OF THIS DATA IN
ORDER TO DECODE, ESSENTIALLY,
THERE ARE PATTERNS OF OUR
BEHAVIOR WE'RE NOT AWARE OF THAT
CAN BE USED TO DECERN WHAT MOST
PEOPLE COULD CREDIT HIGHLY
SENSITIVE INFORMATION.

AND WHEN I TALK I USE THIS
EXAMPLE WITH AUDIENCES ALL THE
TIME.

THEY'RE FLABBERGASTED TO REALIZE
IT'S POSSIBLE WITHOUT EVER YOU
KNOW, IT'S NOT BECAUSE YOU
BOUGHT A HOME PREGNANCY TEST KIT
OR THE OTHER THINGS.

JUST FROM REALLY INNOCENT THINGS
THAT PEOPLE CAN MAKE THESE
GENERALIZATIONS.

WHAT I WANT TO SUGGEST IS THIS
IS THE, THIS IS WHY WHEN PAUL
TAUGZ ABOUT THE DATABASE IT'S
MUCH MORE THAN THE FACTS THAT
YOU INTEND TO DISCLOSE TO
SOMEONE.

IT'S NOT A QUESTION OF HOW
CONFIDENTIAL THAT DATA IS BEING
KEPT.

IT'S ABOUT THE ABILITY TO MAKE
EXTREMELY INTERESTING AND

POWERFUL INFERENCES.
THE DATA IS REMARKABLE AND THE THINGS THAT CAN BE SAID ABOUT A PERSON ARE PROFOUND.
THEY WILL EFFECT IF AN EMPLOYER -- IF TARGET CAN DO THIS THEY CAN SELL THE DATA TO YOUR EMPLOYER.
THE GOVERNMENT CAN USE THE DATA.
THERE ARE ALL OF THESE THREATS THAT COME WITH THE ABILITY TO PIERCE THE VAIL, THE SURFACE VAIL OF FACTS, AND FOR VERY SENSITIVE THINGS ABOUT PEOPLE.
>> I THINK ASHKAN HAD A COMMENT AND THEN MIKE.
>> TWO QUICK POINTS.
I WOULD SAY IT'S THE COLLECTION THAT IS OF CONCERN, TO THE DEGREE WE BROUGHT UP CYBER SECURITY ISSUE.
IF THIS DATA IS COLLECTED.
THE LIKELIHOOD OF BREECH AND SECONDARY USE IT PRESENT, RIGHT.
TO THE LAWYERS IN THE ROOM, YOU WANT TO SK-RBGS AN ODD EXAMPLE YOU HAVE THE OPTION TO HANG A PIANO OVER MY HEAD, IT EXPOSES ME TO HARM IF IT'S NOT TAKEN CARE OF OR PROPERLY SECURED.
WITH COMPANIES COLLECTING THE INFORMATION WITHOUT USER'S KNOWLEDGE THAT COLLECTION EXPOSES THEM TO A BROOCH.
WE SAW THIS WITH BLUE TOAD WHO LEAKED ONE MILLION DEVICE NAMES WHICH CAN BE LINKED TO OTHER INFORMATION ABOUT CONSUMERS.
TO HOWARD'S POINT I AGREE THERE IS AN ADDED SUPPORT ECONOMY, AND VALUE IN THE ECONOMY.
IT'S IMPORTANT TO POINT OUT SOME OF THE BIGGEST PLAYERS IN THE ECONOMY LIKE GOOGLE DIDN'T START THE OBA UNTIL 2007.
PROEUR TO THAT IT WAS CONTEXT

RUL AND SEARCH BASED
ADVERTISING.

EVEN IN THE OBA WORLD WE HAVE TO
SEPARATE INFORMATION THAT USERS
VOLUNTARY KNOW AND GIVE AND
INFORMATION SELECTED ABOUT THEM
TO INFER THINGS.

I PERSONALLY FEEL WE'RE IN A
REALLY, WE'RE IN A GROWING PAINS
TEENAGER AREA OF BEHAVIORAL
ADVERTISING AND TRACKING WHERE
COMPANIES WILL FIND IT'S BETTER
TO ENGAGE A CONSUMER AND ASK FOR
HIGH QUALITY DATA ABOUT THEIR
INTERESTS AND THINGS THEY'RE
WILLING TO SHARE AND LEAVE THE
SENSITIVE THINGS ON THE TABLE
AND NOT INFER THINGS.

WE HAD THIS IN THE MAGAZINE
DAYS.

YOU SIGN UP FOR AUTOMOBILES AND
BIKING WITH YOU MAYBE NOT
DIETING BECAUSE I'M SENSITIVE TO
THAT.

WE ARE WORKING TO MAKE THIS WORK
WITHOUT CREEPY OVER RETENTION OF
ITEMS FOR TIME WITH THINGS
YOU'RE SENSITIVE TO.

>> THE DIFFICULTY OF SAYING
"COLLECTION" SOME OF THE
COLLECTIONS ARE FOR USE THAT'S
ARE INCREDIBLY VALUABLE.

THE PATTERN AN LITTICS HAVE CUT
CREDIT CARD FRAUD RATE BY ABOUT
HALF TO SPOT SUSPICIOUS
TRANSACTIONS THAT MAYBE
FRAUDULENT.

YOU HAVE TO COLLECT THE DATA TO
DO THAT.

YOU ISN'T SAY IT'S CREEPY SHOULD
NOT KNOWS MY CREDIT CARD
PURCHASES BUT IT'S GREAT FOR
THEM TO STOP THE FRAUDULENT USE
OF THE CREDIT CARD.

THOSE ARE TWO SIDES OF THE SAME
COIN.

>> RIGHT.
THE THIRD SIDE OF THE COIN,
DICE.
LET'S GO TO THE D & D WORLD.
THREE SIDED DICE.
YOU COLLECT INFORMATION FOR
FRAUD OR PATTERN DETECTION.
THEN YOU HAVE THE INFORMATION
AROUND.
WOW, THIS IS VALUABLE.
LET ME USE IT FOR MARKETING OR
KEEP IT AROUND FOR A LONG TIME
RISKING BREECH.
>> IF THERE IS A PROBLEM OR USE
THAT'S THE PROBLEM.
>> ONE AT A TIME, PLEASE.
>> WE SHOULDN'T FALL IN THE TRAP
OF USING AT PARTICULAR
TECHNOLOGIES AND TECHNIQUES.
WHAT'S THE HIGHER LEVEL CONCERN
OR PRACTICE.
AN EARLIER WORK SHOT IN THIS
ROOM ON PRIVACY I LEARNED THAT
THE ORIGINAL L.L. BEAN, THE GUY,
GOT HIS START WITH MAIL ORDERER ORDERER
AND SELLING HIS BOOTS BY GOING
TO THE STATE OF MAINE, THE
REGISTRY FOR EVERYONE PURCHASING
A HUNTING LICENSE IN MAINE IN
1908 SOMEWHERE TOOK THAT LIST
AND SENT CIRCULAR ADVERTISING
THE BEST BOOTS FOR HUNTING.
VERY EFFECTIVE.
SAME THING WE'RE TALKING ABOUT
TODAY.
IT'S THE PRACTICE AND THE
CONDUCT NOT THE TECHNOLOGY THAT
WE NEED TO FOCUS ON.
>> WE WANT TO GET EVERYONE
INVOLVED HERE.
SO -- LET ME GET A QUESTION, LET
ME ASK A COUPLE OF QUESTIONS
HERE.
>> I WILL ASK NEIL PARTICULARLY,
ANYONE ELLS FEEL FREE TO CHIME
IN HERE, ARE THERE SPECIAL

CONCERNS ABOUT, YOU KNOW, LET'S FOCUS ON THE COMPREHENSIVE SIDE OF THIS.

THE COLLECTION BECOMES BROADER LOOKING AT MORE THINGS, IS THERE SOMETHING PARTICULAR ABOUT THAT THAT RAISES SPECIAL CONCERNS OR RISKS TO CONSUMERS PRIVACY.

>> DEFINITELY.

I HAVE BEEN TRYING TO KEEP QUIET.

THE FIRST QUESTION WAS BENEFITS. I WAS SITTING ON MY HANDS.

THERE ARE BENEFITS AND THERE ARE TREMENDOUS DANGERS WE NEED TO THINK THROUGH.

I THINK IT BEARS REPEATING THE QUESTION WE HAVE BEEN ASKED. WHAT IS IT ABOUT THE COLLECTION OF DATA, ABOUT ALL OR MOST OF YOUR ACTIVITIES, YOU'RE ALL CONSUMERS, ACROSS MULTIPLE PLATFORMS THAT'S POTENTIALLY PROBLEMATIC?

WE HAVE TALKED A LOT ABOUT IDENTITY THEFT, ONE RISK.

I DON'T WANT TO TALK ABOUT THAT.

I THINK WE HAVE TALKED ABOUT THAT ENOUGH.

I THINK THERE ARE THREE PARTICULAR DANGERS TO FOCUS ON. THE FIRST IS AN IDEA I CALL INTELLECTUAL PRIVACY.

WHEN WE'RE READING, THINKING AND COMMUNICATING WITH FRIENDS AND MAKING SENSE ABOUT THE WORLD USING GOOGLE SEARCH ENGINES USING SILLY, POTENTIALLY EMBARRASSING, OR DEEPLY POLITICAL QUESTIONS THAT, THAT IS DIFFERENT.

WE SHOULD BE PARTICULARLY DANGEROUS ABOUT ACTIVITIES THAT THREATEN OR THAT, THAT CREATE INCENTIVES OR DETER PEOPLE FROM EXPLORING IDEAS.

FROM READING FREELY.
FROM THINKING DEEPLY.
FROM NOT HAVING THAT MOMENTARY
HESITATION.

SHOULD I LOOK UP ON -- MAYBE
IT'S GOOGLE FOR FLU TRENDS.
SHOULD I LOOK ON GOOGLE THIS
FUNNY BUNION I HAVE ON MY
BOTTOM.

I DON'T KNOW IF YOU CAN GET
BUNIONS ON YOUR BOTTOM.

ANYWAYS --

[LAUGHING]

>> YOU MAY BE DETOURING, I WILL
REMAIN SEATED.

YOU MAYBE DETOURING PEOPLE FROM
ASKING QUESTIONS THAT ALSO HAVE
VALUE.

I THINK JUST AS WE CARE ABOUT
FREEDOM OF SPEECH AND WE ARE
CONCERNED ABOUT CHILLING
EFFECTS, PEOPLE EXPRESSING
POLITICAL AND SOCIAL BELIEFS.
SO TOO SHOULD WE BE DEEPLY
CONCERNED ABOUT PEOPLE THINKING,
SEARCHING, READING, AND
EXPLORING TO DETER THEM FROM
THAT.

THE SECOND DANGER HERE I THINK
IS COMPREHENSIVE DATA COLLECTION
AND MASSIVE PROFILING CREATES A
TRANSFORMTIVE POWER CHANGE.

INFORMATION IS POWER, MORE
INFORMATION IS MORE POWER.

IF WE'RE CONCERNED ABOUT
UNCONSCIOUSABILITY AND
SUBLIMINAL ADVERTISING AS WE
HAVE BEEN FOR 50 YEARS, WE
SHOULD BE CONCERNED ABOUT
CHANGES WE'RE MAKING AS A
SOCIETY IN THE POWER
RELATIONSHIPS BETWEEN CONSUMERS
AND BUSINESSES.

FOR EXAMPLE, IT CAN BE USED IF
WE FEEL PARTICULARLY PARANOID,
ABOUT BLACKMAIL.

>> IF I KNOW ABOUT YOU, YOUR
MEDICAL CONDITIONS, POLITICAL
VIEWS.
I CAN BLACKMAIL YOU.
MOST BUSINESSES ARE NOT IN THE
BLACKMAIL BUSINESS, IT'S
ILLEGAL.
A SOFTER FORM OF BLACKMAIL IS
PERSUASION.
IF I KNOW YOUR PREFERENCES AND
WHAT MAKES YOU TICK.
WHAT YOU MIGHT WANT TO DO OR
DOING.
IF I CAN USE BIG DATA TO KNOW
YOU'RE PREGNANT BEFORE YOU KNOW
YOU'RE PREGNANT WHICH IS
POTENTIALLY POSSIBLE.
OR TO KNOW SOMETHING BUT THAT
YOU DON'T KNOW ABOUT YOURSELF,
PREGNANCY TO ONE SIDE.
THEN YOU CAN SELL PEOPLE THINGS
THEY MAY NOT WANT TO BUY.
YOU CAN SHAPE CONSUMER
PREFERENCES.
THIS IS A TREMENDOUSLY POWERFUL.
I AGREE WITH THE OTHER
PANELISTS, SOME OF THE OTHER
PANELISTS THERE ARE GOOD THINGS
HERE.
I THINK WE NEED TO FOCUS ON THE
TRANSFORM TUFF POWER
RELATIONSHIP.
THE OTHER THING THE POWER
RELATIONSHIP CAN BE USED FOR IS
WHAT SOCIAL SCIENTISTS CALL
"SORTING" GROUPING CONSUMERS
INTO CATEGORIES.
MIKE USED THE WORD
"DISCRIMINATION."
ECONOMISTS USE THE WORD
DISCRIMINATION DIFFERENTLY FROM
LAWYERS.
THIS POWER ALSO ALLOWED GENDER
OR DEMOGRAPHIC OR RACIAL OR
ETHNIC OR POLITICAL SEGMENTATION
IN WAYS WE MIGHT FIND

DISTASTEFUL TO SAY THE LEAST.
THE THIRD AND FINAL RISK HERE, I
KNOW THIS IS FOCUS ON BUSINESS,
PRIVATE SECTOR AND GOVERNMENT
BUT THE TECHNIQUES OF
SURVEILLANCE ARE GOVERNMENT AND
COMPANY NEUTRAL.
RIGHT, GOVERNMENTS CAN USE
TECHNOLOGIES TOO.
EVEN IF WE'RE NOT CONCERNED
ABOUT DIRECT GOVERNMENT
SURVEILLANCE THE CREATION OF THE
DATABASES, INTELLECTUAL
PROFILES, HIGHLY GRANULAR
CONSUMER PROFILES TO PREDICT
INDIVIDUAL BEHAVIOR AND LEARN
ABOUT INDIVIDUAL IDENTIFIABLE
PEOPLE IS SOMETHING THAT COULD
BE PARTICULARLY INTERESTED IN
EITHER AS A MARKET PARTNER TO
ADVERTISE, BUYING DATABASES OR LAW
ENFORCE.
, ANTI-TERROR CONTEXT OR HAVING
A LOOK DEPENDING HOW THE REFORM
GOES.
THEY MAY HAVE THE REFORM TOO.
TO JUST HAVE A LOOK AND SEE.
THIS GIVES THE RISK FOR AN
INDIVIDUAL, IT INCREASES THE
POWER OF GOVERNMENT AS WELL.
>> IT BENEFITS GOVERNMENT.
SOMETHING AS SIMPLE AS TRAFFIC
PATTERNS FROM THE VARIOUS
WIRELESS APPS THAT TRACK
PATTERNS HAVE BEEN USED AND ARE
VALUABLE IN LOCAL GOVERNMENTS
IDENTIFYING AND IDENTIFYING
SOLUTIONS FOR TRAFFIC
BOTTLENECKS.
THAT INFORMATION WASN'T AS
EASILY AND READILY AVAILABLE
AS BEFORE.
>> ABSOLUTELY.
I DON'T MEAN TO SAY THIS STUFF
ISN'T USEFUL, THIS ISN'T COOL.
THERE AREN'T LOTS OF USEFUL LIFE

CHANGING THINGS CAN BE USED FROM
OUR DIGITAL REVOLUTIONS AT
LARGE.

BUT TO COLLECT, THIS GOES BACK
TO ASHKAN'S POINT.

TO COLLECT INFORMATION FOR ONE
PURPOSE IS DIFFERENT FROM
COLLECTING INFORMATION FOR ALL
PURPOSES.

I SUSPECT THERE ARE A LOT OF
LAWYERS IN THIS ROOM.

MYSELF INCLUDED.

LAWYERS AND DOCTORS, AS
PROFESSIONALS, ARE VERY GOOD AT
OBTAINING INFORMATION FROM THEIR
CLIENTS AND PATIENTS.

DEEPLY SENSE STITCH -- DAMAGING
INFORMATION.

WE NEED THAT INFORMATION TO FLOW
FROM CLIENTS AND PATIENTS TO
DOCTORS AND LAWYERS SO THEY CAN
TREAT DISEASE, SO THEY CAN GET
THEM OUT OF JAIL.

THEY CAN ADVANCE INTEREST BEFORE
THE FEDERAL TRADE COMMISSION.
NOW WHEN A LAWYER RECEIVES A
CONFIDENCE FROM A CLIENT, THAT
INFORMATION IS USED FOR A
PARTICULAR PURPOSE, FOR THE
CLIENT'S BENEFIT.

IT'S NOT THEN USED FOR MARKET TO
GET CLIENT, TO SELL TO OTHER
MARKETERS, TO THIRD PARTY
MARKETERS.

I THINK IT'S ONE THING TO SAY WE
CAN COLLECT INFORMATION FOR A
PARTICULAR USEFUL PURPOSE.
OF COURSE WE CAN.

IT'S ENTIRELY A DIFFERENT THING
TO SAY THAT INFORMATION NOW
BELONGS TO THE COMPANY.

THE COMPANY CAN USE IT FOR
WHATEVER IT WANTS.

I THINK THE REASON WE HAVE THE
RULES IS BECAUSE THERE IS A
POWER IMBALANCE BETWEEN LAWYERS

AND CLIENTS, DOCTORS AND PRIESTS
AND THE PEOPLE THEY WORK WITH.
WHEN YOU HAVE THAT POWER
IMBALANCE OUR LAW FOR HUNDREDS
OF YEARS HAVE IMPOSED FIDUCIARY
DUTIES.

WHAT WE ARE SEEING A INFORMATION
WE SHOULD TREAT AS A FIDUCIARY.
GOOGLE, ON BALANCE S A FAIRLY
GOOD FIDUCIARY OF PERSONAL DATA
HAS LOTS OF INFORMATION FROM
SEARCH AND ACROSS PLATFORM
ACTIVITIES.

I THINK WE NEED TO INSURE, AS A
SOCIETY, AS SOCIETIES ACROSS THE
WORLD.

THAT INFORMATION THAT IS, THAT
HAS THAT VALUE AND THAT POWER
AND DANGER IS TREAT AD
APPROPRIATELY.

SO WE CAN USE IT FOR THE GOOD
BENEFITS.

DISEASE PREVENTION AND TRAFFIC
KROLL.

WE'RE NOT USING TRAFFIC KROLL
INFORMATION TO ALLOW LAW
ENFORCE.

OR MARKETERS TO FOLLOW US AROUND
IN REAL TIME.

INSTEAD OF A VIDEO VERSION OF
GOOGLE STREET VIEW TO SEE WHAT
IS GOING ON.

I THINK WE NEED TO BE, I DON'T
MEAN TO SOUND PARANOID.

WE NEED TO THINK BROADLY.

YOU ARE CARRYING A DEVICE MORE
POWERFUL THAN CAPTAIN KIRK'S
COMMUNICATOR, 30 YEARS AGO.

PEOPLE WOULD OF LAUGHED.

HOW MANY OF THOSE DEVICES ARE
IN OUR POCKETS, PHONES,
COMPUTERS, VIDEO CAMERAS, STILL
CAMERAS.

WE NEED TO THINK BROADLY INSTEAD
OF LITTLE CASE BY CASE.

TRAFFIC SAFETY IS IMPORTANT, WE

NEED TO DO THAT.
THE FLU IS BAD WE WANT TO SAVE A
COUPLE OF LIVES HERE.
WE NEED TO LOOK AT THE BIG
PICTURE SO WE DON'T MOVE TO A
SOCIETY THAT NONE OF US WANTED
IN THE FIRST PLACE.
>> THE WHOLE POINT IS YOU DON'T
KNOW ABOUT THE BENEFITS UNTIL
YOU LOOK AT THE INFORMATION YOU
COLLECTED FOR ANOTHER USE.
THE INFORMATION YOU USE FOR A
LOCAL TRAFFIC WAS COLLECTED
BECAUSE THE CELLPHONE COMPANY
NEEDED TO KNOW WHERE PEOPLE ARE
IN THE NETWORK.
IT'S ANOTHER USE THAT'S A
VALUABLE USE.
IF THERE ARE BAD USES LET'S
RESTRICT THE BAD USES.
WE HAVE TO FOCUS ON THE USE.
IT'S NOT A PROBLEM THAT THERE IS
LESS CONGESTION ON CITY STREETS
BECAUSE OF INFORMATION SHARING.
IF THERE ARE SENSITIVE
CATEGORIES OF INFORMATION LIKE
THE DOCTOR AND LAWYER EXAMPLE.
I DON'T THINK THAT'S A POWER
IMBALANCE AS MUCH AS THE NATURE
OF THE INFORMATION THAT IS BEING
PROVIDED AND THE NATURE OF THE
SERVICES BEING PROVIDED.
BUT IT DOESN'T MAKE SENSE TO SAY
A DEPARTMENT START IS A
FIDUCIARY.
THAT IS WHAT YOU'RE SAYING.
LET'S NOT USE THAT INFORMATION
FOR ANYTHING BUT THE
TRANSACTION.
>> WHY MAKE THAT THE DEFAULT?
JUST REAL QUICK?
WHY NOT ALLOW PEOPLE, IN SENT I INKEN
INCENTIVIZED PEOPLE TO STEP INTO
THE SYSTEM, I SUSPECT IN A LOST
CASES YOU MIGHT FIND, AGAIN
HIGHER QUALITY INFORMATION FOR

THE PEOPLE WILLING THAT ARE WILLING TO PARTICIPATE AND ACTIVELY.

WE HAVE HAD NEILSON RATINGS FOR AGES.

PEOPLE VOLUNTARILY WANT TO PROVIDE THE INFORMATION AND INCENTIVE.

WE COULD HAVE THE SAME FOR TRAFFIC AND FLU OR WHATEVER ELLS.

>> THE DIFFICULTY WITH THE -- A DEFAULT RULE THAT'S OPTED IN FOR MOST PEOPLE THE QUESTION WHETHER TO ALLOW THE INCIDENTAL USE OF WHERE MY CELLPHONE IS FOR TRAFFIC MANAGEMENT IS SIMPLY NOT WORTH THINKING ABOUT.

THEY HAVE OTHER THINGS TO DO.

THERE ARE EXPERIMENTAL STUDIES THAT INDICATE THE PEOPLE WHO CARE MORE ABOUT PRIVACY ISSUES MAKE CONSISTENT CHOICES.

WHETHER THE OPTION IS OPT IN OR OPT OUT.

THE PEOPLE WHO DON'T CARE DON'T MAKE THE CHOICES, DEFAULT CONTROLS.

IF YOU CARE ABOUT PRIVACY FINE.

IT'S NOT TOO MUCH TO SAY EXPRESS THAT PREFERENCE TO SOMEONE AS OPPOSE TO HAVING US ASSUME YOUR PREFERENCE A PLOYS TO EVERYONE ELLS.

>> THE DIFFICULTY, RETURNING FROM TRAFFIC TO COMPREHENSIVE ON-LINE DATA COLLECTION IS MOST CONSUMERS DON'T KNOW WHAT IS GOING ON.

WHEN THEY SEE THE FACEBOOK LIKE BUTTON ON THE NEW YORK TIMES WEBPAGE THEY DON'T KNOW IF THEY'RE LOGGED INTO THE BROWSER WHICH FACEBOOK MAY SNEAK THAT IN.

THEY WANT TO NUDGE PEOPLE TO

BEING LOGD IN ALL THE TIME.
FACEBOOK KNOWS THEY'RE VISITING
THE WEBSITE.
CONSUMERS DO NOT KNOW THE LEVEL
OF THE TRACKING.
WHEN, WHEN, YOU KNOW, IT'S
EXPLAINED TO THEM THEY'RE
SHOCKED.
I THINK IT'S ENTIRELY DIFFERENT
TO SAY WE SHOULD HAVE ANALYTICS
THAT CAN MONITOR TRAFFIC
CONGESTION.
YOU CAN HAVE AN ANONYMOUS
TRAFFIC METRICS.
THEY DON'T NEED TO KNOW IT'S ME
AT THE STOP LIGHT, NECESSARILY
TO PREDICT THE TRAFFIC PATTERN.
THEY CAN SAY THAT'S A CAR.
THAT'S ABSOLUTELY FINE.
I THINK HOWARD IS CONFLATING
DIFFERENT KINDS OF DATA USAGE.
WITH RESPECT TO THE ON-LINE
STUFF I THINK THE BOOKS YOU
READ, WHAT SEARCHES YOU MAKE OF
SEARCH ENGINES.
THOSE ARE DEEPLY, DEEPLY
SENSITIVE KINDS OF INFORMATION.
I THINK IF YOU'RE TO ASK
CONSUMERS, I THINK PEOPLE V OF
COURSE THEY DON'T WANT PEOPLE TO
KNOW WHAT THEY HAVE BEEN READING
OR WHAT THEY HAVE BEEN ASKING OR
WHAT THEY'RE WONDERING ABOUT.
I THINK THE DIFFICULTY SETH THE
DEFAULT IN WAY THAT'S DO TAKE
ADVANTAGE OF THE BENEFITS
WITHOUT SAYING EVERYTHING GOES.
IF YOU CARE ABOUT IT, IF YOU'RE
A WEIRD PRIVACY FREAK YOU HAVE
TO OPT IN.
HONESTLY WE WILL GIVE YOU -- YOU
HAVE TO OPT OUT.
WE WILL HIDE IS THAT OPT OUT.
IT'S IN THERE SOMEWHERE IN THE A
ADENDUMS CONSTANTLY CHANGING
PRIVACY POLICIES.

>> LET ME ASK A QUESTION.
YOU'RE TALKING ABOUT TRACKING
BOOKS AND READING.
IS THERE ACTUALLY A COMMERCIAL
INTEREST IN THAT TRACKING RIGHT
NOW?

IS THIS SOMETHING THAT IS OF
INTEREST TO BUSINESSES IN
ANYWAY?

>> AMAZON CLEARLY DOES IT.
AND CONSUMERS LOVE IT.

>> SO, A CONTEXT, A QUESTION OF
CONTEXT FOR US.

LET ME DIRECT SOMETHING OVER TO
LEE THEN.

WE HAVE BEEN TALKING ABOUT DEPTH
OF INFORMATION.

LET'S COMBINE THE SUBJECTS.

IS THERE A DANGER OF COMBINE
-PING A FACEBOOK WITH DEEP SET
OF INFORMATION YOU LARGELY
VOLUNTEER WITH YOUR LIKES AND
DISLIKES, CONNECTIONS WITH
BROADER INFORMATION FROM OTHER
SITES.

YOUR WEB BEHAVIOR AND PLACES YOU
GO, PLACES YOU THINGS YOU BUY
AND KINDING THE INFORMATION.

DOES THAT PROVIDE SPECIAL RISKS
TO CONSUMERS?

>> I DON'T THINK IT'S SPECIAL
RISKS.

IT'S A QUESTION OF GREATER SCALE
AND GREATER MAGNITUDE.

WHAT WE SEE HERE IS -- WELL, I
GUESS THE WAY I THINK ABOUT IT
IS ONCE AS INFORMATION IS STORED
IT WILL HAVE A TENDENCY TO
AGGREGATE TOGETHER.

THERE ARE TREMENDOUS FINANCIAL
INCENTIVES TO DO THAT.

THERE ARE NON FINANCIAL
INCENTIVES TO DO THAT.

IT'S A BIT LIKE IN THE SECOND
TERMINATOR MOVIE, I THINK.

YOU BLOW THAT THING UP BUT ALL

OF THOSE BITS OF SILVER AND METAL ALWAYS COME BACK TOGETHER AGAIN.

IT'S ALMOST AN IRON LAW UNDER OUR PRESENT SITUATION THAT THE DATA WITHOUT REGULATION, WITHOUT SOME VERY, VERY STRONG TECHNICAL SILOING, THE THE TECHNICAL DATA COLLECTED ABOUT PEOPLE WILL AGGREGATE TOGETHER.

THIS OBVIOUSLY, NEIL DID A GREAT JOB OF TALKING ABOUT FRAMES AND HOW WE WANT TO THINK ABOUT THESE PRIVACY HARMS.

I THINK THAT THE, I WANT TO ADD TO THAT, HE'S ABSOLUTELY RIGHT. THE ULTIMATE QUESTION IS SORT OF ONE OF POWER AND ONE OF FAIRNESS.

I THINK WE TEND TO BE LOOKING FOR EXAMPLES OF INDIVIDUAL HARM OR HOW A INDIVIDUAL MIGHT BE HARMED AS A RESULT OF SOMETHING.

AT THE SAME TIME WE FRAME THE BENEFIT AND LOOK AT THE BROAD PUBLIC GOOD TYPE BENEFITS THAT CLEARLY COULD EXIST.

AT THE END OF THE DAY TO ME THERE IS A THREAT MODEL.

ONE IS THE ENTITIES THAT HAVE AND CAN AGGREGATE THE DATA. THEY'RE NOT YOU.

AND YOUR INTERESTS.

THE CONSUMER'S INTEREST IS NOT THE THING THAT THEY ARE SEEKING TO MAXIMIZE IN OUR SYSTEM.

WHAT WE ARE, WE HOPE IN OUR MARKET ORIENTATED SYSTEM THAT THE FRAMEWORK AND THAT INCLUDES THE LAWS AND REGULATIONS WILL SHAPE EVERYONE'S SELF INTEREST IN A WAY THAT WE ACTUALLY COME OUT COLLECTIVELY AHEAD.

IN A SITUATION LIKE WE HAVE RIGHT NOW, WHERE IT'S REALLY OBVIOUS THAT CONSUMERS DO NOT

KNOW WHAT OR HOW DATA IS BEING COLLECTED ABOUT THEM.
WHO IS COLLECTING THAT DATA.
HOW IT IS BEING USED AND WHAT.
I WILL KEEP GOING BACK TO THE EXAMPLE.
WHY I THINK IT'S FOLLY TO TRY TO SEPARATE SENSITIVE FROM NONSENSE NONSENSITIVE DATA.
IF THEY CAN FIGURE OUT SENSITIVE INFORMATION FROM WHAT YOU BUY AT THE STORE.
THERE IS NO WAY TO SAY THIS IS SENSITIVE AND THIS IS NOT.
IT'S ALL ANALYZABLE.
THE SCALE WHICH YOU AGGREGATE IS ONE THAT ALLOWS FOR BETTER AND BETTER MINING AND PATTERN RECOGNITION IN THESE DATABASES.
THAT CAN BE, IF YOU, IF THE INCENTIVES ARE NOT FOR THE CONSUMER THAN THEY WILL BE FOR SOMETHING ELLS.
THOSE CAN BE GOVERNMENT SURVEILLANCE, THOSE CAN BE EMPLOYER SURVEILLANCE, THOSE CAN BE A WHOLE LOT OF THINGS THAT ARE GOING TO BE, MAKE IT VERY, VERY DIFFICULT FOR, FOR INDIVIDUALS.
THE FACT THAT THE TECHNOLOGY CHANGES ALL THE TIME.
IT BECOMES MORE EFFECTIVE AT BOTH ANALYZING AND INFERENCING AND COLLECTING, MEANS THAT THE DEMOCRATIC PROCESS IN WHICH TO THE EXTENT THAT POLITICS DOES REFLECT IN SOME WAYS WHAT PEOPLE KNOW ABOUT A PROBLEM.
HOW THEY UNDERSTAND IT.
HOW THEY WANT TO FIX IT.
I THINK YOU END UP WITH A POLITICAL MARKET FAILURE THERE AS WELL.
FRANKLY ONE OF THE THINGS I WORRY ABOUT IN THIS WORLD OF

MICRO TARGETING IS THAT BECAUSE SO MUCH ELECTORAL POLITICS NOW HAS BECOME MORE TIED TO THIS KIND OF DATA GATHERING AND ANALYTICAL TARGETING TO THAT, IT WILL BE DIFFICULT FROM, IN A WASHINGTON D.C. TYPE ENVIRONMENT TO WEAN THE POLITICAL WORLD AWAY FROM THE BENEFITS OF THIS. IT'S NOT JUST A QUESTION OF CORPORATIONS BENEFITING FROM IT. BUT IF, POLITICIANS REALIZING THAT THEIR ABILITY IS TIED TO, SOMETHING THAT THEY WILL VALUE VERY MUCH. I SEE SERIOUS PROBLEMS LOOK AGO HEAD.

>> I THINK THAT BRINGS UP ANOTHER QUESTION, I WILL DIRECT THIS TO MARKHAM INITIALLY. ANYONE CAN JUMP IN AFTERWARDS. CONSUMERS NOT UNDERSTANDING THE COLLECTIONS GOING ON. AS FAR AS YOU HAVE SEEN WHEN COMPANIES USE A COMPREHENSIVE DATA COLLECTION TO INTEGRATE AND CREATE NEW SERVICES HOW MUCH ARE THEY THINKING ABOUT USER PRIVACY WHEN THEY DESIGN IT? IS IT PART OF THE DESIGN PROCESS OR IS IT THOUGHT ABOUT AFTERWARDS.

>> MORE AND MORE THE NORM, ESPECIALLY WITH BIGGER INTERNET FLAT FORMS AND INTERNAL AND EXTERNAL PRIVACY COUNCIL IS FULLY INTEGRATED WITH PRODUCT DEVELOPMENT SO PRIVACY CONSIDERATIONS ARE THOUGHT OF AT EVERY STAGE OF A SERVICE OR PRODUCT BEING DEVELOPED. THAT'S PROBABLY A GOOD THING. I THINK THOUGH THAT THE ISSUE OF COLLECTION VERSUS HARM ISSUE IS A IMPORTANT ONE. ULTIMATELY MOST OF THE EXAMPLES

WE HEAR IF THIS HAPPENS AND THIS HAPPENS AND THIS HAPPENS THEN THIS IS THE HARM . SO, I THINK IT'S NECESSARY FOR US TO FOCUS IN THE POLICY FACE ABOUT WHAT HARMS WE SEEK TO ADDRESS. THAT'S ULTIMATELY WHERE, WHERE WE LAND IN TERMS OF TALKING ABOUT OUR CONCERNS. IT'S WHY I THINK THE COLLECTION ITSELF FOCUSING ON THE COLLECTION ITSELF IS ALMOST A IMPOSSIBLE TASK TO COME UP WITH A RULE THAT FOCUSES ON THE COLLECTION ITSELF. UNLESS WE'RE GOING TO SAY TKHR THEREIS A INHERENT PROPERTY RATE TO DATA, THE DATA ITSELF. IN THE UNITED STATES WE TAKE A TORQUE BASED APPROACH. WHAT HARMS RESULT FROM THE USE OF DATA? THAT'S A FUNDAMENTAL DISTINCTION THAT GETS DEFLATED. >> I WANT TO SECOND THAT. I THINK THAT THE ISSUE ISN'T WHAT CONSUMERS KNOW. CONSUMERS HAVE NO IDEA WHAT HAPPENS IN THE BOOT SEQUENCE TURNING ON THE COMPUTER. THEY'RE REASONABLY CONFIDENT IT WON'T BLOW UP, THEY WORRY WHY IT TAKES SO LONG THAT IRRITATES THEM. THEY DON'T NEED TO KNOW. THERE IS NO REASON FOR THAT INFORMATION. IF YOU THINK CONSUMERS SHOULD BE BEHAVING DIFFERENTLY THEN YOU SHOULD PERSUADE CONSUMERS TO BEHAVE DIFFERENTLY. THAT'S WHAT WE DO WITH EVERYTHING ELLS. YOU SHOULDN'T GET THE GOVERNMENT TO SAY DO IT THIS WAY, THIS IS HOW WE DO IT.

>> I NEED TO CHIME.

IN SECOND, THIRD, FOURTH
SOMEWHERE OUR MEMBERS, WE
REPRESENTED SERVICE PROVIDERS
NOW BROADLY REPRESENT SERVICE
PROVIDERS AND WIRELESS DATA
SERVICES HAVE INCORPORATED THE
PRIVACY BY DESIGN CONCEPTS.
THEY DO HAVE PRIVACY POLICIES.
THEY HAVE ADOPTED THEM AS
CONSUMER BEST PRACTICES.
THEY CREDIT THE CONSENSUS AND
NOTICES.

WE WILL HEAR FROM LORI KRAMER
THIS AFTERNOON.

I DON'T PRETEND TO HAVE THE
EXPERTISE THAT SHE AND OTHERS
HAVE IN TERMS OF WHAT CONSUMERS
UNDERSTAND.

IN THE MARKETPLACE THERE ARE
CERTAINLY RESPONSES TO THE
CONCERNS GIVING CONSUMERS FAR
MORE CHOICE THAN THEY HAD A YEAR
AGO OR TWO YEARS AGO.

JUST YESTERDAY'S NEW YORK TIMES
HAD A STORY ABOUT WIRELESS TEXT
MESSAGING, AND THE DEVELOPMENT
OF NEW ALTERNATIVES FOR
CONSUMERS LIKE AN APP THAT
DOESN'T PRESENT EVEN CONTEXTUAL
ADVERTISING.

FOR THOSE CONSUMERS THAT PREFER
THAT KIND OF SERVICE IN THE
BROWSER WORLD.

FIRE FOX HAS A VERY DIFFERENT
KIND OF CONSUMER EXPERIENCE THAN
SAY CHROME DOES OR INTERNET
EXPLORER.

SO, WE ARE SEEING IN THE
MARKETPLACE THE DEVELOPMENT OF
CHOICES AND THE CHOICES MUST BE
BASED ON THE FACT THAT CONSUMERS
ARE INTERESTED IN THE SERVICES.

>> CAN I JUMP IN WITH THREE
QUICK POINTS.

THE FIRST IS THE OBVIOUS

COLLECTION CONSTRAINTS ARE NOT THE ONLY TOOL HERE THAT WE HAVE. ONE OF THE, ONE OF THE OTHER TOOLS IS TO SIMPLY DISCARD AND DESTROY THE DATA ONCE IT HAS BEEN USED FOR, FOR THE ORIGINAL PURPOSE.

THIS IS, YOU KNOW WHEN WE TALK ABOUT DO NOT TRACK, IN THAT DISCUSSION WE HAVE BEEN TALKING ABOUT, WELL, YOU COULD ALLOW LONGER RETENTION FOR A LONG PERIOD OF TIME OF DATA TO DEAL WITH THE -- PROBLEM OR SOMETHING LIKE THAT.

THEN AT SOME POINT THERE IS A VERY CLEAR DESTRUCTION OF THE DATA. THERE ARE WAYS.

IT'S NOT JUST SAYING DON'T COLLECT.

IT'S MORE NUANCE THAN THAT.

A SECOND, ONE OF THE DISTINCTIONS WE HAVE BEEN USING FOR A LONG TIME IS THE NOTION OF VOLUNTEERED SORT OF CONSENTED DISCLOSURE OF DATA VERSUS TO NON.

YOU WERE TALKING, YOU ASKED HOW THE THINGS MIX TOGETHER.

ONE OF THE THINGS I WORRY ABOUT IS THIS DISTINCTION IS GOING TO MATTER LESS AND LESS.

THIS IS BECAUSE OF DYNAMIC EFFECTS.

THERE IS A PROFESSOR, A COLLEAGUE OF PAUL HOLMES THAT HAS TALKED ABOUT THE UNRAVELING EFFECT.

THE UNRAVELING EFFECT ON PRIVACY IS ONE IN WHERE BECAUSE SOME CONSUMERS MAY HAVE GOOD DRIVING RECORDS OR GOOD CREDIT SCORES OR WHATEVER, THEY HAVE A INCENTIVE TO DISCLOSE THAT IN ORDERER TO GET A BENEFIT.

THEN WHAT HAPPENS IS THAT ANY

ONE WHO TRIES TO MAINTAIN
PRIVACY ABOUT A MATTER LIKE
THAT, THEY AUTOMATICALLY HAVE A
NEGATIVE INFERENCE.

YOU KNOW IF YOU'RE APPLYING FOR
SCHOOL AND THE PEOPLE WITH THE
GOOD GRADES SENT IN TRANSCRIPTS
AND EVERYONE ELSE DOESN'T.

WELL, OBVIOUSLY THE FACT THAT
YOU DIDN'T SUBMIT A TRANSIT
MEANS YOU.

YOU END UP WITH A POWERFUL
DYNAMIC OVERTIME THAT NO MATTER
HOW MUCH YOU DON'T WANT TO SAY
SOMETHING THERE IS A STRONG
INCENTIVE TO DISCLOSE.

IS THIS SORT OF DYNAMIC EFFECT
IN THE AREA OF DISCLOSURE, I
THINK, IT'S GOING TO CHANGE AS
THE CHARACTER OR CHANGE THE WAY
WE THINK ABOUT WHAT IS
VOLUNTEERED INFORMATION.

IT IS MORE VOLUNTEERED UNDER,
UNDER A KIND OF DURESS
SITUATION.

>> WE HAVE A QUESTION FROM THE
AUDIENCE I WANT TO ASK.

THEN I HOPE WE CAN SWITCH GEARS
A LITTLE BIT AND TALK ABOUT
SPECIFIC TECHNOLOGIES.

THE QUESTION IS TO HOWARD'S BOOT
UP EXAMPLE.

WHAT IF THE OPERATING SYSTEM WAS
INSTALLING SPYWARE PART OF THE
BOOT PROCESS, THINGS SO
UNEXPECTED SHOULD THEY BE
DISCLOSED TO THE CONSUMER.

>> NO MAKE THE OPERATING SYSTEM
STOP INSTALLING SPYWARE.

THIS ISN'T A NOTICE PROBLEM.

THIS IS A INSTALLATION OF
SOFTWARE YOU DIDN'T WANT.

THE PROBLEM ISN'T THAT I DIDN'T
KNOW.

IF THE BOOT SEQUENCE THERE IS A
GROWING STRING OF TEXT OVERTIME

AS IT TELLS ME ABOUT THE THINGS
SOMETHING THOUGHT I SHOULD CARE
ABOUT, THAT IS HAPPENING.

SOMEWHERE IN THERE IS THERE A
LINE THAT SAYS I'M INSTALLING
SOFTWARE THAT WILL WIPE YOUR
HARD DRIVE.

I DON'T THINK THAT DISCLOSURE
SOLVES THE PROBLEM.

>> THAT'S MORE OF A MATTER OF
PRIVACY BY DESIGN TO BLOCK
THAT --

>> MORE OF A MATTER OF ENFORCE.
ENFORCEMENT.

>> I'M A LITTLE CONFUSED.

IF I UNDERSTAND THE QUESTION
RIGHT.

IF THE OPERATING SYSTEM ITSELF
COLLECTS DATA LIKE SPYWARE.

IT RECORDS YOUR CLICK STREAM,
YOUR BROWSING ACTIVITY.

WHAT IS YOUR RESPONSE THERE
THERE?

SORRY, IS THAT OKAY?

IT'S NOT THIRD PARTY SOFTWARE.

THIS IS THE FUNCTION OF THE
OPERATING SYSTEM MUCH LIKE A
MOBILE DEVICE UNDER VERIZON
RECORDS YOUR CLICK STREAM AND
LOCATION ACTIVITY.

WHAT WOULD BE THE APPROPRIATE
STANDARD THERE.

>> THERE IS NO POINT AS WE HEARD
THIS MORNING IN TRYING TO HAVE A
ONSCREEN DISCLOSURE THAT SAYS
THIS IS ABOUT WHAT IS TO HAPPEN
IN A CIRCUMSTANCE WHERE YOU GOT,
WHERE THERE IS NOTHING IN THE
WORLD YOU CAN DO ABOUT IT EXCEPT
GET A DIFFERENT OPERATING
SYSTEM.

THAT'S THE LEVEL WHICH THE
COMPETITION HAS TO OPERATE.

THE OPERATING SYSTEM WILL
COLLECT THE INFORMATION IT
COLLECTS.

I DON'T KNOW WHAT IT HAS ON THERE.

IN, IN THE NORMAL OPERATION OF MY COMPUTER IT HAS ALL SORTS OF HISTORY FILES BECAUSE I CAN FIND THINGS WHEN I LOST THEM.

>> SURE.

>> WHICH IS A GOOD THING.

I DON'T KNOW WHAT INFORMATION IT IS DOING THERE.

I DON'T WANT TO KNOW.

>> SO, IF THERE -- MOST OF THE OPERATING SYSTEM IN THE MARKETPLACE COLLECTS AND TRANSMITS THAT INFORMATION AND IT'S NOT DISCLOSED OR MARKET DIFFERENTIATION WITH THE OPERATING PROVIDERS.

WHAT IS YOUR RECOMMENDATION FOR THE OUTCOME OF THAT SCENARIO?

HOW DO YOU ADDRESS THE ISSUE YOUR OPERATING SYSTEM COLLECTS AND DISTRIBUTES THE INFORMATION NOT FOR NEEDING TO WORK BUT OTHER PURPOSES LIKE IN THE CASE OF VERIZON?

>> THAT IS A QUESTION WHICH, WHICH CAN ONLY AT THE END OF THE DAY BE RESOLVED IN THE MARKETPLACE.

>> IF THE MARKETPLACE FAILS --

>> THERE IS NO FAILURE IN THE MARKETPLACE.

THERE IS NO DIFFERENTIATION. THERE IS NO DIFFERENTIATION IN CONSUMER PREFERENCES.

>> IF THERE ARE NOT ENOUGH CONSUMERS TO SUPPORT, OKAY. THE KIND OF NECK KNOWLEDGE GEE YOU WOULD LIKE, THE APPROACH YOU WOULD LIKE IT WON'T SURVIVE IN THE MARKET.

YOU CAN'T BUY THREE WHEEL CARS NO MATTER HOW MUCH YOU WANT.

>> WE WILL GET INTO THE COMPETITION LEVEL IN THE NEXT

PANEL.

LET'S MOVE FORWARD.

WE HAVE OTHER THINGS TO COVER.

ONE THING I WANT TO ASK ABOUT IS

IN THE COMMISSION'S MARCH

PRIVACY REPORT AS COMMISSIONER

POINTED OUT THIS MORNING.

WE TALKED ABOUT THE HEIGHTENED

PRIVACY CONCERNS ASSOCIATED WITH

ISPs USING DEPAC INSPECTION

FOR MARKETING PURPOSES.

YESTERDAY THERE WAS A PRESS

RELEASE ABOUT THE NEW VERIZON

SELECTS PROGRAM THAT VERIZON

WIRELESS IS LAUNCHING.

IT SEEMS THAT UNDER THIS, THIS

PROGRAM VERIZON WILL TARGET

ADVERTISING BASED ON THE

CUSTOMER DATA USAGE INCLUDING

WEB BROWSING AND USE OF MOBILE

APPS.

SPRINT HAS AN AD BASED ON

CONSUMER ACTIVITIES ON MOBILING

DEVICES.

HOW DO WE SEE KPREP HEN SIEVE

DATA COLLECTION IN THE SMART

PHONE CONTEXT.

>> THIS IS -- WITHOUT INTERNET

YESTERDAY.

>> I SPEAK I HOPE AUGUST ORE IT

A IT A TIFFLY FROM SECONDHAND

NOTHING OR FROM MY PHONE.

IN OUR OFFICE EVERYONE USED

THEIR SMARTPHONE AND HOT SPOTS

TO TETHER LAP TOPS TO GET TO THE

INTERNET.

BUT THIS IS A SERVICE AS I

UNDERSTAND THAT IS OPT IN.

AND YOU KNOW IT'S A CONTEXTUAL

SERVICE, SIMILAR TO THE KIND OF

SEARCH ENGINE QUEARY INFORMATION

THAT IS, YOU KNOW, BEING DONE

ELSEWHERE IN THE ECOSYSTEM.

>> ALRIGHT.

I'M GOING TO GO AHEAD.

WE'RE A LITTLE TIGHT FOR TIME.

I WANT TO MOVE ONTO A COUPLE OF QUESTIONS.

I HAVE ONE FROM TWITTER TO ASK REAL QUICK.

I WANT TO GET AUDIENCE QUESTIONS ANSWERED.

THIS IS ABOUT COLLECTING AGAIN.

THIS PERSON WONDERS IF ANOMNYZING THE DATA AT COLLECTION WOULD SOLVE CONCERNS AND WOULD THIS ALLOW THAT.

>> I WOULD SAY IT WOULD SOLVE MANY OF THE CONCERNS.

THIS ISN'T -- WORKDAY.

MAYBE IT IS.

PAUL HAS SHOWN ENMITY CAN BE RECONSTRUCTED.

CERTAINLY THINGS YOU CAN DO, THINGS COMPANIES CAN DO TO COLLECT THE INFORMATION IN A RESPONSIBLE PRIVACY RESPECTABLE WAY IS GOOD.

I WAS BE WILDERED BY HOWARDS COMPUTER ANALOGY.

GETTING PRIVACY QUESTIONS IN AT THE DESIGN STAGE RATHER THAN PRIVACY BEING A SORT OF A MARKETING DENIAL THING OR A WAVING OF THE HANDS.

AND REALLY NOT DOING ANYTHING. PRIVACY, IF IT'S MEANINGFUL AND BROUGHT INTO BUSINESS PRACTICES.

IF IT IS BROUGHT INTO THE DECISION, IDEALLY IF THERE IS MARKET COMPETITION ON PRIVACY. THESE, THESE WOULD ALL BE GOOD THINGS.

ANOMYIZATION AND ENGINEERING PRIVACY AND EMBEDDING IT HEPSZ.

IT'S THE SENSITIVE QUESTIONS BY ENGINEERS AND COMPANIES, CHIEF PRIVACY OFFICERS THAT CAN HELP US GET MANY, MOST, MAYBE ALL MOST OF THE BENEFITS OF THESE KINDS OF TECHNOLOGIES WITHOUT CREATING A LOT OF THESE PRIVACY

RISKS AND HARMS.

>> WE SEE THE MARKET INTRODUCING MORE ENCRYPTED APPS ASSOCIATED WITH FINANCIAL SERVICES AND THE LIKE.

THE ENTERPRISE AREA.

USE OF VIRTUAL PRIVATE NETWORKS IS A GOOD WAY OF PROVIDING MORE SECURE COMMUNICATIONS ON TOP OF THAT WITH ENCRYPTION.

SO THAT, AS THE TECHNOLOGIES AND THE SERVICES EVOLVE AS PEOPLE RECOGNIZE THE IMPORTANCE OF SECURING THE COMMUNICATIONS, SECURING THE PRIVACY OF IT. WE SEE THESE FEATURES AND FUNCTIONS BUILT IN.

AT THE SAME TIME WE HEAR FROM WHRAU ENFORCE.

THEIR FRUSTRATION AND GETTING ACCESS TO THIS CONTENT.

>> I WANT TO ADD YOU WANT TO BE CAREFUL HOW YOU USE THE WORD "ANONYMOUS DATA" IT'S NOT A FAIRY DUST THAT RENDERS IT HARMLESS.

THERE ARE A LOT OF EXAMPLES OF COMPANIES CLAIMING ANONYMOUS DATA. I HAVE PERSONALLY REIDENTIFIED THAT DATA OR PSEUDO A DENT FIRE TO USER SOCIAL NETWORKS.

THERE WAS A INSTANCE I WAS ABLE TO TAKE OVER PEOPLES SPACE BOOK AND TWITTER ACCOUNTS USING AN ANONYMOUS A DENT FIRE.

TO THE IDEA YOU CAN USING THAT TERM YOU WANT TO MAKE SURE IT'S BEDDED IN THE COMPUTER SCIENCE WORD "ANONYMOUS" THAT'S ALWAYS AN EVOLVING STANDARD.

>> IF I CAN JUMP IN TO.

I THINK THIS IS SOMETHING THAT HAS TO BE PART OF THE TOOL KIT.

I WOULD NEVER SUGGEST IT'S SIMPLY A PANACEA FOR THE

TECHNICAL REASONS WE KNOW ABOUT.
IT'S IN THE AREA OF ON-LINE
TRACKING, SUCH AS DO NOT TRACK,
ONE OF THE BIG FIGHTS, I WON'T
SAY FIGHTS.

ONE OF THE BIG DISCUSSIONS WE
HAVE HAD, SOMETIMES I'M MORE
HONEST THEN OTHERS.

BIG DISCUSSIONS WE HAVE HAD OVER
HOW YOU HANDLE THIS DATA NEEDED
FOR SECURITY OR CLICK FRAUD, AT
THE SAME TIME WANTING TO
MITIGATING THE PRIVACY CONCERNS
HAS BEEN THROUGH TRYING TO
FIGURE OUT CAN WE USE A UNLINK
ABILITY METRICS.

CAN WE SAY, 1024 UNLINK ABILITY
AS A WAY TO HAVE, HAVE BUCKETS
THAT DON'T RESOLVE IN A GRAN AOU
HRAR FUNCTION BUT FROM A
TARGETING PERSPECTIVE.

IF YOUR COOKIE, AS WE SAW IN
DAN'S PRESENTATION HOW HIGHLY
PERSISTENT UNIQUE IDENTIFICATION
IS BEING USED THROUGHOUT
BOTH THE OFF-LINE AND ON-LINE
WORLD WITH -- BUT IF YOUR COOKIE
STATES FOR -- PREFERENCES,
GARDENING, AIR TRAVEL, HAWAII,
AND YOU KNOW LANGUAGE ENGLISH.
YOU KNOW PERHAPS THAT CAN ALLOW
FOR THE ADVERTISING WITHOUT EVER
ACTUALLY COMPROMISING THE, THE
IDENTITY OF THE INDIVIDUAL THE
WAY THAT --

A 16 LETTER OR NUMBER STREAM
WOULD.

>> ALRIGHT.

THANK YOU.

LET ME, WE ARE GOING TO MOVE
ONTO ANOTHER KIND OF MORE
SPECIFIC TOPIC.

ONE OF THE THINGS THAT
COMMISSIONER TALKED ABOUT.
WHAT STARTED THE MOVE TO THE
WORK SHOP IS THE DISCUSSION OF

DPI.
WHY WE WANT TO LOOK AT THE KNOCK
KNOWLEDGE GEEZ IN A BROADER
QUESTION.
DPI REMAINS AS SORT.
POSTER CHILD OF THE BIG BAD WOLF
OF THIS AREA IN A LOT OF PEOPLES
MINDS.
I WANT TO SPEND A COUPLE OF
MINUTES TALKING ABOUT THAT.
WHAT EXACTLY IS DPI USED FOR.
WHAT CAN IT SEE.
WHAT ARE THE LIMITS OF LOOKING
AT USERS, WHAT CAN IT ACTUALLY
GET FROM A USER'S ACTIVITY?
IF, YOU KNOW ASHKAN IF YOU WOULD
LIKE TO START WOULD I LOVE TO
HEAR FROM EVERYONE.
>> THIS IS TO EXAMINE NOT JUST
THE HEADER INFORMATION.
THE HEADER IS THE ROUTEING
INFORMATION WHO DESCRIBES WHO
THE ENVELOPE IS TOO.
IMAGINE A ENVELOPE IN THE MAIL
SYSTEM THIS IS THE OUTSIDE OF
THE ENVELOPE.
DPAC LOOKS FOR THE CONTENT IN
THE ENVELOPE.
THE USER INFORMATION, CONTENT OF
THE WEB SITES, PASS WORDS,
COOKIES, ETCETERA.
DEPENDING ON THE TECHNOLOGY USED
THERE ARE DIFFERENT LIMITATIONS.
FOR EXAMPLE, UNLESS MY ISP LAS A
DEAL WITH A SIGNING PROVIDER
THEY CAN NOT DECRYPT MY TRAFFIC
CRYPTED WITH MY ABILITY.
CORPORATIONS INCLUDING I THINK
THE FDC HERE THEY USE BLUE COAT
BLUE COAT AS PART OF THE SET UP
PROCESS YOUR IT ADMINISTRATOR IN
STALLS THE CERTIFICATE ON YOUR
DESK TOP OR LAPTOP THAT ALLOWS
THAT TO DESCRIPT THE HTTP AND
HSTP TRAFFIC.
THEY'RE ABLE TO LOOK AT ANYTHING

KNOWING ON THE WIRE NOT CRYPTED
WITH A SECOND TECHNOLOGY.
YOU CAN USE THEN VPN TO TUNNEL
THAT.

IF I USE A STRONG ENCRYPTION
WITH THE VPN THEN THE ONLY THING
THE ISP CAN SEE IS.

THEN I HAVE TO TRUST THE VPN
PROVIDER THEY'RE NOT INSPECTING
THE TRAFFIC AND DATA.

SAME WITH TOR.

THERE ARE LOTS OF ISSUES WHERE
PEOPLE WILL INSTALL MALICIOUS
SOFTWARE ON TOR EXIT NOTES AND
MONITOR YOUR TRAFFIC THERE.

THERE IS A GOOD ARTICLE FROM
BRUCE SNIDER A COUPLE OF WEEKS
AGO.

HE MADE A TALK THIS LAST YEAR
ABOUT KIND OF THE RETURN OF
FUTILISM AND TRUSTING CERTAIN
ENTITIES OR OTHER ENTITIES.

AT SOME POINT SOMEONE HAS TO
CARRY MY TRAFFIC.

UNLESS ALL OF THE WEB SITES I GO
TO SUPPORT HT -- I AM VULNERABLE
TO WHO IS CARRYING MY TRAFFIC.

YOU HAVE TO TRUST SOMEONE.

YOU MAY TRUST YOUR PROVIDER,
AT&T, YOUR LOCAL ISP OR
WHATEVER.Oz IS

ULTIMATELY YOU STILL ARE EXPOSED
TO SOMEBODY AND YOU HAVE TO,
LIKE, LET SOMEBODY CARRY YOUR
TRAFFIC OTHERWISE YOU CAN'T
CONNECT WITH THE INTERNET.

>> AND THE REALITY IS THAT ALL
OF US ROUTINELY USE LOTS OF
DIFFERENT SERVICE PROVIDERS.

SO -- YOU KNOW, AT OUR WORKPLACE
WE'LL HAVE ONE ADDRESS AND
IDENTITY AND SERVICE PROVIDER.

ON OUR WIRELESS DEVICES WE'LL
HAVE ANOTHER ONE.

AT HOME WE'LL HAVE YET A THIRD.

YOU CAN THEN DIRECT ANY OF THOSE

THROUGH V.P.N. OR APPS IN DIFFERENT PATHS THAN INTENDED SO ROUTINELY ALL OF US WITH SMART PHONES IN THIS ROOM HAVE A CHOICE OF EITHER THE COMMERCIAL RADIO FREQUENCIES OR THE F.C.C.'S WI-FI NETWORK AS A PROVIDER.

SO THE CONCEPT OF A COMPREHENSIVE ONE STOP SHOP TO CAPTURE PERSONAL INFORMATION FROM ALL THE DATA THAT WE SEND AND RECEIVE IS NOT ACCURATE.

THESE TECHNOLOGIES AND TECHNIQUES, THOUGH, DO HAVE MANY OF THE SAME CHARACTERISTICS.

>> THERE WAS A CASE, THOUGH, LIKE -- AN EXAMPLE WITH -- I THINK IT WAS PUBLICLY DISCLOSED WITH SPRINT AND THEIR COMPANY CALLED -- THEY WERE USING AN ANALYTICS COMPANY CALLED CARRIER I.Q. WHICH WOULD MONITOR YOUR TRAFFIC ON THE DEVICES FOR THE PURPOSE OF IMPROVING SERVICE. THEY WERE ABLE TO MONITOR YOUR BROWSING HABITS NOT JUST WHEN YOU WERE ON THE SPRINT NETWORK, BUT WHEN YOU WENT HOME TO YOUR WI-FI AND CONNECT THROUGH YOUR LOCAL WI-FI THEY STILL WOULD COLLECT THAT INFORMATION AND PROVIDE THAT.

SO I FEEL LIKE, YES, TO SOME DEGREE BUT, AGAIN, AT EACH STEP OF THE GAME YOU'RE EITHER TRUSTING YOUR HAND SET, YOU'RE TRUSTING YOUR I.S.P., YOU'RE TRUSTING YOUR KEYBOARD OR YOU'RE TRUSTING YOUR BROWSER.

AT SOME POINT EACH ONE OF THOSE ENTITIES HAS THE ABILITY TO MONITOR YOUR USAGE AND TO THE DEGREE THAT YOU USE SOMETHING LIKE SINGLE SIGN ON, EITHER YOUR CREDIT CARD OR YOUR USER NAME,

YOUR E-MAIL ADDRESS, ANY IDENTIFIER, THAT ACTIVITY CAN BE LINKED ACROSS ALL OF THOSE DIFFERENT NETWORKS.

>> AND WHEN THESE STORIES BREAK IN THE NEWS AND THE INFORMATION IS MADE CLEAR TO CONSUMERS, THE ATTENTION THAT THESE STORIES GET SHOWS CONSUMERS REALLY DO CARE ABOUT COMPREHENSIVE TRACKING ACROSS PLATFORMS.

>> THE SLIDES I HAVE GO TO THIS QUESTION OF THE FRAGMENTATION OF PEOPLE'S USE OF -- OF WHERE THEY'RE ONLINE AND HOW THEY'RE ONLINE.

IF THIS WOULD BE A GOOD TIME TO DO THOSE FOR 60 SECONDS?
OKAY.

>>

I APOLOGIZE TO THOSE ON THE WEB CAST BECAUSE THESE APPARENTLY AREN'T ON THE -- ON THE OFFICIAL SLIDE DECK.

I'M IN A BUSINESS SCHOOL AND THE NUMBER-ONE THING WE TEACH STUDENTS IN FINANCE IS DIVERSIFY TO REDUCE YOUR RISK AND THAT'S WHAT'S HAPPENING IN THE ONLINE MARKETPLACE.

CONSUMERS USING MULTIPLE DEVICES MULTIPLE NETWORKS, MULTIPLE BROWSERS FROM MULTIPLE LOCATIONS AND ENCRYPTION IS GROWING AND ALL OF THESE REDUCE VISIBILITY INTO CONSUMER BEHAVIOR.

MULTIPLE DEVICES.

THIS IS DATA FROM Q.

13% OWN A LAPTOP, A SMART PHONE, AND A TABLET.

OBVIOUSLY THE PAIR WISE OVERLAP IS MUCH HIGHER.

A 2010 SURVEY THAT PEW DID, THE AVERAGE PERSON UNDER 45 OWNS FOUR INTERNET-CAPABLE DEVICES. OR LIKELY INTERNET-CAPABLE

DEVICES.

ALL OF THOSE ARE USED FOR BROWSING IN DIFFERENT WAYS. CONSUMERS USE MULTIPLE NETWORKS. THIS IS, I THINK SORT OF REALLY STRIKING.

THE EXTENT TO WHICH PEOPLE MIX WI-FI AND MOBILE ACCESS AND HOW IT DIFFERS ACROSS DEVICES.

OVERALL IN 37% OF THE TRAFFIC FROM PHONES GOES VIA WI-FI IN THIS RECENT STUDY.

SO EVEN WHERE IT'S GOING OVER DIFFERENT -- OVER DIFFERENT NETWORKS.

PEOPLE USE MULTIPLE BROWSERS. THAT'S NOT NECESSARILY A CHOKE POINT, EITHER, AND BROWSER MARKET CHANGES REMARKABLY QUICKLY.

I PICKED 2010 AND 2012 BECAUSE IT'S THE COMMISSION'S DRAFT REPORT AND ITS FINAL REPORT AND INTERNET EXPLORER'S MARKET SHARE FELL 20% AND CHROME'S DOUBLED.

THIS IS A DYNAMIC MARKETPLACE WITH LOTS OF PEOPLE USING LOTS OF DIFFERENT BROWSERS.

AND PEOPLE BROWSE FROM FROM LOTS OF DIFFERENT LOCATIONS.

THE CHART ON THE LEFT IS N.T.I.A. DATA ON WHERE PEOPLE BROWSE AND THIS IS SORT OF A USUAL ACCESS KIND OF QUESTION 40% HOME, 27% WORKPLACE.

9% COFFEE SHOPS, CAFES.

THE CHART ON THE RIGHT IS A RECENT GOOGLE STUDY THAT LOOKS AT THE DAILY MEDIA INTERACTIONS AND ASKS HOW MANY OF THEM WERE INSIDE THE HOME AND HOW MANY WERE OUTSIDE ON A COMPUTER, 31% OF DAILY INTERACTIONS ARE OUTSIDE THE HOME.

ON A PHONE, 40% OF THE DAILY INTERACTIONS ARE OUTSIDE THE

HOME.

ON A TABLET ABOUT 21% THAT ARE OUTSIDE OF THE HOME.

SO THERE'S THIS MIX OF HOME AND NOT AT HOME THING.

AND FINALLY ENCRYPTION.

IT'S NOT SOME VERY FREQUENTLY TRAFFICKED SITES, INCLUDING FACEBOOK AND GOOGLE AND TWITTER HAVE ADOPTED ENCRYPTION AT VARIOUS LEVELS AS PART OF THE DEFAULT FOR SOME OF THEIR SERVICES.

IN PART FOR SECURITY REASONS BUT IT ALSO MEANS THAT IT'S A LOT HARDER TO READ THAT TRAFFIC.

SO I THINK IT IS -- THERE'S NOT ANYBODY WITH A SINGLE COMPREHENSIVE VIEW.

THE QUESTION IS THE EXTENT TO WHICH YOU CAN MAKE LINKAGES ACROSS THE DIFFERENT CHANNELS THAT CONSUMERS ARE USING.

BECAUSE CONSUMERS REALLY HAVE DIVERSIFIED THEIR RISKS.

>> THANK YOU.

WE HAVE A QUESTION THAT WAS RAISED IN THE AUDIENCE AND I WANT TO GO AHEAD AND -- WE JUST HAD A QUICK QUESTION ABOUT THE SLIDES WHICH I DIDN'T GET -- I COULDN'T SEE THEM FROM HERE BUT I'M SURE I AGREE WITH EVERYTHING ON THEM, I'M SURE.

(LAUGHTER)

THE QUESTION I HAD IS IN YOUR EXAMPLE, FOR EXAMPLE, DIFFERENT LOCATIONS AND DIFFERENT I.S.P.s, HOW MANY OF THOSE CONSUMERS WOULD USE THE SAME COMMON SERVICES LIKE FACEBOOK OR GOOGLE TO LINK THAT ACTIVITY?

DID YOU LOOK AT THAT AT ALL OR DO YOU HAVE ANY THOUGHTS?

>> I DON'T KNOW.

IT'S CLEAR IF YOU LOG INTO A

FACEBOOK OR GOOGLE YOU'LL BE ABLE TO LINK ACROSS DEVICES. THAT'S CLEARLY POSSIBLE. BUT, YOU KNOW, THE THING ABOUT THAT KIND OF TRACKING IS YOU CAN LOG OUT ANY TIME YOU WANT. THE OPT OUT IS RIGHT THERE AND EASY.

>> SO SOME OF MY RESEARCH HAS SHOWN THAT, IN FACT, YOU CAN'T OPT OUT ANY TIME YOU WANT BECAUSE SITES WILL PLACE PERSISTENT COOKIES SUCH THAT PREVENT YOU FROM OPTING OUT. ADDITIONALLY, THE COOKIES WOULD ALLOW YOU TO LINK MULTIPLE BROWSERS SO EVEN WHEN YOU WENT FROM I.E. TO FIREFOX AND SWITCH BROWSERS THEY'RE THE SAME PERSISTENT IDENTIFIERS THAT WOULD ALLOW THEM TO IDENTIFY THE SAME CUSTOMER ACROSS MULTIPLE BROWSERS.

SO PERHAPS NOT.

>> NONE OF THESE ARE PERFECT SEPARATIONS.

I'M NOT TRYING TO SAY THAT. YOU CAN OBVIOUSLY MAKE LINKAGES BUT THERE'S NOBODY THAT'S SITTING ON A CHOKE POINT THAT EVERYTHING GOES THROUGH AND THAT HAS COMPREHENSIVE PICTURE OF WHAT'S GOING ON.

>> WITH REGARD TO THE QUESTION ABOUT DEEP PACK INSPECTION, YOU KNOW, THE TECHNOLOGY ITSELF IS NOT A BAD TECHNOLOGY IT'S USED FOR A LOT OF GOOD THINGS, INCLUDING TO PREVENT CYBER ATTACKS AND OTHER THINGS. AND THE CONCERN THAT'S BEEN RAISED BY T.P.I. IS IT'S A SERVER THAT TENDS TO BE AT THE END POINT OF THE NETWORK SO IT DOES LITERALLY COLLECT EVERYTHING COMING THROUGH THE

NETWORK.

AGAIN, THAT'S HOW IT WORKS.
BUT IT'S THE USE OF THE D.I.P.
SERVER THAT'S RAISED THE
CONCERN.

AND IN THE CONTEXT IN NEBUWEB,
BECAUSE IT CAN LOOK AT ALL THE
COMMUNICATIONS, I THINK THEY
WERE ADVERTISING THAT THEY COULD
SEND THAT TO AN ADVERTISER AND
AS YOU PULLED UP YOUR WEB
BROWSER YOU WOULD GET AN AD THAT
WOULD BE BECAUSE OF THE CONTENT
OF THAT COMMUNICATION AS IT WAS
BEING DELIVERED LIVE.

AND THERE WERE A LOT OF CONCERNS
THAT WOULD VIOLATE WIRETAP LAWS,
AMONG OTHER THINGS.

SO, AGAIN, I KEEP COMING BACK TO
THIS COLLECTION ISSUE, BUT THE
TECHNOLOGY ITSELF, I THINK, WE
SHOULD BE CAREFUL NOT TO
DEMONIZE THE TECHNOLOGY BUT
RATHER, AGAIN, GOING TO USES.

>> IF I COULD JUST SECOND THAT
BECAUSE IT'S ONE OF THE
INTERESTING IRONIES OF
CONTROVERSY ABOUT DEEP PACK AND
INSPECTION THAT THE COMMISSIONS
MICROSOFT CASE FROM 2002 ON THE
SECURITY ISSUES SPECIFICALLY
ALLEGES THAT, AMONG OTHER THINGS
THAT WERE SECURITY DEFICIENCIES,
WAS THE FAILURE TO DO
INSPECTIONS TO PROTECT THE
NETWORK.

>> LET ME GET TO THAT QUESTION
THAT WE GOT FROM THE AUDIENCE
BECAUSE IT IS CORRECTED TO THIS
QUESTION -- THIS POINT YOU WERE
MAKING ABOUT THE FRAGMENTATION
OF PEOPLE GOING TO DIFFERENT
PROVIDERS AND THROUGHOUT THE DAY
AND THE QUESTION IS ARE THE
MULTIPLE OPTIONS THAT YOU'VE
DESCRIBED AVAILABLE THROUGHOUT

THE U.S.?

WHAT ABOUT DEEPLY RURAL AMERICA?
IS THERE SOME CON CONSTRICTION
OF OPTIONS AVAILABLE TO FOLKS
DEPENDING ON WHERE IN THE
COUNTRY YOU ARE?

>> I CAN SPEAK TO WIRELESS
NETWORKS.

THE FEDERAL COMMUNICATIONS
COMMISSION AS WELL AS THE C.T.I.
WEB SITE HAS SOME VERY GOOD DATA
ABOUT THE NUMBER OF AMERICANS
WITH CHOICES OF FIVE OR MORE
CARRIERS, FOUR OR MORE CARRIERS,
THREE OR MORE CARRIERS SO THAT
ALL BUT 1% 20%, PROBABLY THE
DIFFERENT 1% 20%, THAT ALL BUT
1% OR 2% OF AMERICANS DO HAVE
THE CHOICES OF THEIR WIRELESS
SERVICE PROVIDER.

>> WHICH I THINK IS GREAT.

AND TO ECHO THAT POINT, TWO OF
THE FOUR MAJOR CARRIERS ARE
CURRENTLY ENGAGING IN THIS TYPE
OF COLLECTION.

SO YOU HAVE TWO CHOICES.

YOU SHOULD MAKE CHECK -- AND
IT'S UNCLEAR, ACTUALLY, I KNOW
T-MOBILE DOES D.P.I. FOR NETWORK
MANAGEMENT.

THEY HAVEN'T ANNOUNCED THAT
THEY'RE DOING IT FOR ADVERTISING
AND TRACKING.

IT WOULD BE FUN TO CHECK IN NEXT
YEAR ABOUT THIS TIME AND SEE OF
THOSE FOUR IF THE OTHER TWO ARE
STILL NOT ENGAGED IN THIS
PRACTICE.

>> I THINK ON THE POINT ABOUT
TECHNOLOGY, D.P.I. HAS SOME
VALID USES.

IT'S LIKE A GUN OR A CAR OR A
KITCHEN KNIFE.

WE CAN USE THEM FOR GOOD OR FOR
BAD.

BUT THE IMPORTANT POINT IS TO

FOCUS ON THAT.

IS TO BE SURE THAT YOU DON'T USE
-- JUST BECAUSE D.P.I. HAS GOOD
USAGE DOESN'T MEAN THAT IT'S
FINE AND FOR ALL THINGS AND ALL
PURPOSES.

I THINK THERE MAY BE TARGETED
USES FOR THE TECHNOLOGY BUT THAT
DOESN'T MEAN TECHNOLOGIES DON'T
CONTAIN RISKS.

WE SHOULD BE MINDFUL ABOUT THE
POWER OF THESE TECHNOLOGIES.
THE SAME WAY WE ARE MINDFUL OF
THE POWER OF GUNS.

WE DON'T GET TO BRING GUNS INTO
THE F.T.C. CONFERENCE CENTER.
I WAS TOLD I HAD TO LEAVE MINE
OUTSIDE.

BUT WE LIKE TO HAVE GUNS
REGARDLESS OF ONES POLITICS IF
FOR NO OTHER REASON WE LIKE
HAVING A MILITARY AND THOSE
FOLKS HAVE GUNS AND D.P.I. IS
LIKE THAT.

IT'S ONE THING TO SAY D.P.I. CAN
BE USED FOR NETWORK MAINTENANCE
AND SECURITY ISSUES.

IT'S QUITE ANOTHER THING TO SAY
D.P.I. IS A TECHNOLOGY FOR ALL
SEASONS.

>> I THINK D.P.I. SOMEHOW HAS
BEEN DEMONIZED.

I THINK THE LARGER LESSON-- AND
I BELIEVE THERE'S A CONSENSUS
FROM ALL OF US WHO HAVE
PARTICIPATED SO FAR TODAY-- THAT
RATHER THAN LOOK AT A TECHNOLOGY
WE SHOULD LOOK AT CONDUCT AND
PRACTICES.

BECAUSE COOKIES, THE SOCIAL
PLATFORMS, THE CONCERNS THAT WE
ALL SHARE IN TERMS OF PROTECTING
PRIVACY ARE -- GO ACROSS
TECHNOLOGIES AND BY FOCUSING ON
D.P.I. OR COOKIES OR ANY OTHER
SINGULAR -- SINGLE CHOKE POINT

OR TECHNOLOGY YOU REALLY MISS
THE COMPLEXITY, THE DIVERSITY
AND THE IMPORTANCE LOOKING AT
THE -- PHI PHIING THE CONDUCT
THAT YOU WANT TO POLICE AND
PROTECT.

>> THAT RAISES A GOOD QUESTION.
DEEP EYE IS A POWERFUL TOOL AND
CAN GIVE YOU A LOT OF INSIGHT.
ARE THERE OTHER TECHNOLOGIES
THAT GIVE YOU THE SAME INSIGHT
AND IS THERE SOME WAY TO LOOK AT
WHAT IS MOST INVASIVE OR USEFUL
THAT WILL TELL US IS IT JUST AN
AMOUNT OF INFORMATION OR THE
TYPE OF INFORMATION.

HOW DO WE LOOK AT THIS AND
DECIDE WHAT IS MOST TROUBLING?

>> I'D JUST MAKE AN INITIAL --
FROM A POLICY MAKING STANDPOINT
TRYING TO LOOK AT A POLICY
SOLUTION THROUGH A SPEFK LENS OF
TECHNOLOGY IS PROBLEMATIC.
TECHNOLOGIES CHANGE QUICKLY WHAT
DEEP YAY DOES NOW, OTHERS MAY DO
IN THE FUTURE.

SO WE'VE BEEN TRYING TO AVOID
TECHNOLOGY SPECIFIC SOLUTIONINGS
SO I THINK THE EXERCISE ABOUT
LOOKING AT DIFFERENT
TECHNOLOGIES MIGHT BE USEFUL IN
SOME CONTEXT BUT TRYING TO CRAFT
A SOLUTION BASED ON THAT IS I
THINK PROBLEMATIC.

>> I THINK I WOULD AGREE I
COMPLETELY AGREE THAT FOCUSING
ON A SPECIFIC TECHNOLOGY IS NOT
USEFUL IN THIS CONTEXT.

YOU CAN BREAK IT INTO THE TYPES
OF INFORMATION -- I THINK DAN
MADE A GOOD POINT AT LOOKING AT
INFORMATION FLOWS.

SO JUST TO PUSH BACK ON -- SOME
PEOPLE WOULD ARGUE THAT D.P.I.
IS NOT AN OKAY TECHNOLOGY.
THERE'S A SCHOOL OF THOUGHT

WHICH IS LIKE THE SANCTITY OF THE COMMUNICATION THAT THE MIDDLE LAYER SHOULD BE DUMB AND YOU CAN DO MOST OF THE TRAFFIC SHAPING AND NETWORK MANAGEMENT FEATURES WITHOUT UNPACKING THE ENVELOPE.

YOU CAN DELIVER MAIL WITHOUT SCANNING INSIDE THE ENVELOPE. SOME PEOPLE FEEL THAT, ESPECIALLY WITH S.S.L. BUT WITH REGARDS TO WHAT KIND OF OTHER TECHNOLOGIES OR WHAT THE INFORMATION FLOWS THAT TECHNOLOGY PROVIDES SO YOUR MONITOR, KEYBOARD AND MOUSE HAVE ACCESS TO YOUR INTERACTIONS, RIGHT?

BUT WE HAVEN'T TO SYSTEM DEGREE -- EXCEPT FOR KEY LOGGERS WE HAVEN'T SEEN THINGS LOOKING AT THAT INFORMATION.

THEN COMES YOUR OPERATING SYSTEM.

YOUR OPERATING SYSTEM HAS MAYBE USED MULTIPLE DEVICES BUT YOUR OPERATING SYSTEM HAS VISIBILITY INTO ALL OF YOUR TRAFFIC AND ACTIVITY AND BEHAVIOR.

WE'VE BEEN GOOD IN THAT REGARD. WE HAVEN'T SEEN OPERATING SYSTEMS ON THE DESKTOP SIDE COLLECT TOO MUCH USER INFORMATION WITH THE EXCEPTION OF LIKE RECENTLY THERE WAS SOME OBUNTU SENT YOUR SEARCH HISTORY TO AMAZON AND I THINK WE'LL SEE MORE OF THESE AS THE OPERATING SYSTEMS MOVE TO A CLOUD-BASED INTERACTION.

ESPECIALLY IN THE MOBILE ARENA WHERE MOBILE DEVICES TRANSMIT YOUR INFORMATION TO THE MOBILE CARRIERS BEYOND THAT.

THERE'S THE BROWSERS. THE BROWSER MAKERS HAVE BEEN

GOOD ABOUT NOT CAPTURING ALL OF YOUR TRAFFIC SOME WILL CAPTURE CLICK STREAM HISTORY.

GOOGLE HAS A FEATURE THAT ARE SYNC YOUR TABS ACROSS MULTIPLE DEVICES SO WHEN YOU'RE ON YOUR TABLET AND DESKTOP YOU CAN SEE WHAT TABS ARE OPEN AND READ THE SAME CONTENT.

IN FACT, THAT TRACKS ALL OF YOUR BROWSER HISTORY BECAUSE IT HAS TO KEEP TABS -- KEEP TRACK OF WHAT TABS ARE OPEN.

THEN AFTER THE BLOUZER COMES BROWSER PLUG INS.

SURPRISINGLY -- DAN WAS MAKING A POINT OF AD BLOCK AND STUFF.

THESE PLUG INS HAVE ACCESS TO ALL OF YOUR TRAFFIC.

IF YOU ENABLE THE GHOST RANK FEATURE IT WILL TRANSMIT ALL OF YOUR BROWSING HISTORIES SO EVERY SET YOU GO TO SO THAT TRANSMITS IT BACK TO GO STREET.

SO -- IT'S IMPORTANT NOTE THAT THESE ALL HAVE VISIBILITY INTO YOUR TRAFFIC.

IF THEY WANTED TO IF THEY WERE DELICIOUS ONE DAY THEY COULD CAPTURE EVERYTHING YOU TYPE OR READ.

THEN YOU GET TO THE I.S.P. WHICH IS WHAT THIS DISCUSSION HAS BEEN -- OR D.P.I., WHICH IS THE CARRIER ITSELF CAN ACTUALLY VIEW MOST OF THE TRAFFIC EXCEPT S.S. AND IN SOME CASES THEY CAN VIEW S.S.L. THEN YOU GET INTO THIS IDEA THAT THIRD PARTIES THAT AREN'T ON YOUR DEVICE BUT ARE ABLE TO CORRELATE YOUR ACTIVITY ACROSS YOUR DEVICE ALSO HAVE VISIBILITY NOT JUST TO YOUR BROWSING HISTORY BUT I DON'T KNOW IF YOU'VE USED THESE COPY AND PASTE MECHANISMS THAT LETS

YOU COPY TEXT OFF THE "NEW YORK TIMES" AND PASTE IT IN E-MAIL, THEY GET THAT CONTENT THAT YOU'VE COPIED AND GENERATE THIS UNIQUE U.R.L..

THERE HAVE BEEN SOME CASES OF MORE MALICIOUS ONES THAT WILL SCAN THE CONTENT OF POST BUS FOR THE MOST PART THE THIRD PARTY IS MAINTAINING VISIBILITY TO YOUR BROWSING HISTORY AND TO THE ANSWER OF HOW YOU CARVE IT OUT, I THINK YOU CARVE IT OUT IN A SIMPLE WAYS WHICH LIKE LOW AMOUNTS OF VERY SENSITIVE INFORMATION OR HIGH AMOUNTS POTENTIALLY THAT COVER A WIDE PORTION OF YOUR LIFE.

THIS IS KIND OF LIKE TOUCHING ON U.S. V. JONES WHICH IS YOU CAN SAY THAT IT'S INVASIVE OR AGGRAVATION OF A LOT OF DIFFERENT TOUCH POINTS ABOUT A PERSON'S ACTIVITY.

I DON'T THINK THERE'S A CLEAR STANDARD THERE.

THE QUESTION IS HOWEVER FRAGMENTED THE COLLECTION MIGHT BE, THE PRODUCT IS DATA ABOUT THE PERSON.

>> AND IF YOU BELIEVE IN THE TERMINATOR APPROACH, THEN THAT DATA IS GOING TO FLOW SOMEPLACE AND BECOME MORE SDRALIZED SO AT THE END OF THE DAY I THINK IT'S MUCH MORE -- WHILE IT'S IMPORTANT TO UNDERSTAND THE SIZE OF THE ATTACK SURFACE THEN WHAT ASHKAN HAS DESCRIBED IS A VERY LARGE ATTACK SURFACE, THE BIG PART OF THE QUESTION IS ARE WE GOING TO ALLOW THAT DATA TO AGGREGATE REGARDLESS OF WHETHER IT'S COMING FROM ONE POINT, THREE POINTS OR 29 POINTS. IF IT'S AGGREGATING SOMEWHERE

AND THEN BEING USED WITH NO RESTRICTIONS WE HAVE A PROBLEM PROBLEM.

>> THE QUESTION I HAVE NOW, AND THIS GOES BACK TO WHAT COMMISSIONER BRILL REPORTED THIS MORNING.

IN THE COMMISSION'S REPORT AND PRIOR TO THAT IT GOES BACK TO OUR ONLINE BEHAVIORAL ADVERTISING PRINCIPLES, WE'VE DRAWN A DISTINCTION BETWEEN FIRST PARTY INTERACTIONS AND THIRD PARTY INTERACTIONS?

WE'VE SAID WITH RESPECT TO MARKETING IN MOST CASES FIRST PARTY MARKETING IS SOMEWHAT TRANSPARENT TO AN INTUITIVE TO THE CONSUMER.

AND WE'VE MADE A DISTINCTION WHERE THE DATA COLLECTION THAT'S BEING USED FOR MARKETING IS HAPPENING BEHIND THE SCENES BY A THIRD PARTY THAT THE CONSUMER MIGHT NOT BE AWARE OF.

AND WE SAID THAT WHERE IT'S FIRST PARTY THE COLLECTION AND MARKETING IS TYPICALLY GOING TO BE PART OF THE CONTEXT OF THE CONSUMER'S INTERACTION WITH THE BUSINESS OR THE RELATIONSHIP THE QUESTION IS DOES THAT PARADIGM WORK WHEN WE'RE TALKING ABOUT COMPREHENSIVE DATA COLLECTION AND FOR EXAMPLE TO GO BACK TO THE I.S.P./D.P.I. CONTEXT, I HAVE A RELATIONSHIP WITH MY I.S.P. FOR THEM TO GIVE ME BROAD BAND SERVICE.

DO I -- AS PART OF THAT, IS IT CONSISTENT WITH MY INTERACTION WITH THAT I.S.P. THAT THEY'RE GOING TO TRACK ME ACROSS WEB SITES?

>> MET ME WEIGH IN ON THE CONSEQUENCE BECAUSE THE TRACKING

ACROSS WEB SITES IS GOING TO LEAD TO AN ADVERTISEMENT. IT IS CERTAINLY CONSISTENT WITH YOUR SUBSCRIPTION TO THE "WASHINGTON POST" THAT THEY'RE GOING MARKET TO YOU. THE MARKETING IS VERY MUCH PART OF THAT RELATIONSHIP. THAT RELATIONSHIP USES INFORMATION ABOUT THE NATURE OF THE POST'S SUBSCRIBERS SO I DON'T KNOW WHAT'S DIFFERENT ABOUT THE SUBSCRIPTION RELATIONSHIP WITH AN I.S.P. AND THE SUBSCRIPTION RELATIONSHIP WITH A MAGAZINE OR A NEWSPAPER THAT IS GOING TO GIVE YOU ADVERTISING.

>> WELL, FROM WHAT WE'VE HEARD TODAY, COMPARING WHAT THE NEWSPAPER WOULD KNOW ABOUT ME BASED ON MY ADDRESS AND WHAT AN I.C.P. CAN KNOW ABOUT WHAT I DO ONLINE IS -- I'M NOT SURE THAT MASHES UP TOO WELL.

>> BUT THAT IS SAYING THAT THE HARM ITSELF IS KNOWING AND I DON'T THINK THAT IS A DEFENSIBLE PROPOSITION.

THE HARM HAS TO BE SOME CONSEQUENCE OF HOW THAT INFORMATION IS USED. AND IF THE ONLY USE YOU'RE WORRIED ABOUT IS MARKETING, THAT HAPPENS ALL THE TIME AND CONSUMERS EXPECT IT.

>> AND TO THE EXTENT THAT CONSUMERS DON'T LIKE IT-- AND WE'VE SEEN THIS WITH CHANGES IN TERMS OF SERVICE ON FACEBOOK AND OTHER SITES.

THEY LET THEIR VIEWS BE KNOWN VERY, VERY QUICKLY. SO WE'VE COME A LONG WAY IN THE LAST FEW YEARS IN TERMS OF SOPHISTICATION NOT JUST AS

INDUSTRY PROFESSIONALS BUT AS
USERS AND WHAT -- AND, OF
COURSE, THE NORM CONTINUES TO
EVOLVE ALONG WITH THE TECHNOLOGY
AND ALL OF OUR EXPERIENCES WHEN
SOME OF THESE APPLICATIONS AND
USES GET AHEAD OF THE NORM
THERE'S A LOT OF PUSHBACK WHICH
IS A GOOD THING.

>> I GUESS I DON'T GET THE
ANALOGY BECAUSE I THINK THAT A
LOT OF PEOPLE SAID "THIS IS LIKE
THE PHONE COMPANY LISTENING TO
MY PHONE CALLS" WHICH IS
SOMETHING THAT THE AVERAGE USER
OF PHONE SERVICE SIMPLY DOESN'T
EXPECT.

THE IDEA IN THAT RELATIONSHIP IS
THAT THEY ARE ACTING PRETTY MUCH
AS A CONDUIT AND NOT PAYING
ATTENTION TO THE CONTENT OF
THOSE THINGS WE HAVE RULES UNDER
THE WIRETAP ACT THAT MAKE IT
VERY CLEAR THAT THE ROLE OF THAT
KIND OF SERVICE PROVIDER IS NOT
TO LOOK AT -- NOT TO ACQUIRE
CONTENT WITHOUT VERY VERY
SPECIFIC AUTHORIZATIONS.

SO I THINK THAT THAT'S VERY
DIFFERENT FROM, SAY SUBSCRIBING
TO A MAGAZINE OR A NEWSPAPER.
WHERE YOU ARE RECEIVING CONTENT
FROM THEM IN THE TRADITIONAL
ADVERTISING.

I DO NOT SEE THE ANALOGY THERE.

>> IF WE'RE TALKING ABOUT -- ONE
COULD ARGUE WE DON'T HAVE A
CONTEXT OTHER THAN THE WAY
THINGS ARE.

IF A CONTEXT BECOMES THE WAY
THINGS ARE, CONTEXT IS NOT
PROVIDING ANY CHECK ON THE
ABILITY OF THIS KIND OF ACTIVITY
TO OCCUR.

IF YOU'RE TALKING ABOUT READING,
WE HAVE CON K.P. TEXTS OF

READING.

WHEN YOU READ A -- NOT THAT WE DO VERY MUCH ANY MORE BUT IT'S ABOUT NEWSPAPERS.

YESTERDAY THERE ARE ADVERTISEMENTS IN PAPER NEWSPAPERS BUT THE NEWSPAPER ISN'T LOOKING BACK AT YOU WHEN YOU'RE LOOKING AT IT.

THE PAPER ONE ISN'T.

THE ELECTRONIC NEWSPAPER IS.

IF YOU EXPLAIN THAT TO A CONSUMER WHICH IS WHY WE HAVE THESE PRIVACY PANICS EVERY FEW MONTHS PEOPLE DO GET NERVOUS. THINK THINK THERE IS A DANGER, THEY DO BELIEVE THEY CAN'T CONTEXTUAL INTEGRITY OF THEIR RELATIONSHIP HAS BEEN VIOLATED SO I THINK IT'S VERY DANGEROUS FOR US TO FOR THE F.T.C. TO SAY CONTEXT ALONE IS WHAT WE DO.

I THINK THAT CONTEXT IS VERY MUCH TIED TO OLD ANALOGIES, PHONE COMPANIES, BOOKS, LIBRARIES, NEWSPAPERS RATHER THAN MEDIA THAT LOOKS BACK AND TRACKS AND TARGETS AND PROFILES.

>> I THINK THERE'S SOME VALUE THERE.

I AGREE WITH NEIL.

BUT THE MODEL INSTEAD OF KIND OF BOOKS AND NEWSPAPERS, WE MIGHT JUST PUT IT AROUND PEOPLE.

PEOPLE WE KNOW AND DON'T KNOW. PEOPLE WE'RE ENGAGING WITH, INTERACTING WITH AND, AS DAN PUT IT, EVERYONE ELSE.

AND I THINK THE SIMILARITIES BETWEEN THINGS LIKE D.P.I. AND THIRD PARTY ADVERTISING IS THAT IN THE CONTEXT OF D.P.I. AND THE CONTEXT OF PROLIFIC THIRD PARTY ADVERTISING THERE'S PEOPLE THAT I'M INTERACTING WITH THAT MIGHT BE THE "WASHINGTON POST" OR THE

"NEW YORK TIMES" OR THE "WALL STREET JOURNAL" THAT'S SERVING ME ADS AS I'M READING THEIR CONTENT.

BUT THERE'S A HANDFUL OF PEOPLE THAT I DON'T KNOW ABOUT, DON'T HAVE A RELATIONSHIP WITH THAT MONITOR MY ACTIVITY ON THAT -- ON THE "WASHINGTON POST" OR THE "NEW YORK TIMES."

AND MAYBE THAT'S OKAY BECAUSE THEY PROVIDE THE ADS, BUT THOSE SAME PEOPLE ALSO MONITOR ME ON THE OTHER SIDE.

SO I GO TO THE "NEW YORK TIMES", THE SAME PERSON THAT I DON'T KNOW WILL MONITOR ME ON THE "WALL STREET JOURNAL" AND ON WHATEVER OTHER SENSITIVE SITE, WEB M.D. THAT I GO TO AND THEY LINK THAT ACTIVITY AND I THINK THAT AGGREGATION ACROSS THESE DIFFERENT CONTEXTS OF PEOPLE THAT I DON'T KNOW IS WHAT THE SENSITIVITY IS.

IF IT WAS EACH OF THE FIRST PARTIES, IF I ENGAGE WITH FACEBOOK AND FACE BOOKS NOSE A LOT ABOUT ME, AT LEAST I'M AWARE OF WHAT THEY THOUGH ABOUT ME. IF I ENGAGE IN GOOGLE AND THEY KNOW ABOUT ME, AT LEAST I KNOW THE TYPE OF INFORMATION AND FUNNY ENOUGH NEITHER ARE HERE TO DISCUSS IT-- WHICH IS GOOD TO POINT OUT-- BUT IT'S THE FACT THAT -- EVEN WHEN I'M NOT ENGAGING WITH FACEBOOK, WHEN I'M ENGAGING WITH THE "NEW YORK TIMES" OR THE "WASHINGTON POST," FACEBOOK LEARNS MORE ABOUT ME OR GOOGLE LEARNS MORE ABOUT ME THAT I THINK IS OF CONCERN AND I THINK THAT'S WHY THIS FIRST-PARTY/THIRD-PARTY DESCRIPTION IS HELPFUL.

>> WELL, IT'S IMPORTANT TO KEEP IN FRONT OF MIND THAT WHILE WE NEED TO BE AWARE, SENSITIVE TO THE SENSITIVITIES IN TERMS OF POLICIES AND PRESCRIPTIONS, WE REALLY REMAIN FOCUSED ON THE HEART.

SO FOR ALMOST ANYTHING WE CAN IMAGINE CONCERNS AND FACTORS THAT WE NEED TO BE SENSITIVE TO WE WANT TO POLICE THE HARMS WE CAN IDENTIFY.

>> I HAVE A POLICY OF NOT INVITING MY MOM OUT ON DATES WITH ME.

AND PART OF THE REASON IS I DON'T WANT HER SHOWING PHOTOS OF ME AS A KID TO THIS NEW PERSON I'M INTERESTED IN.

>> YOU CAN'T STOP IT.

>> I CAN'T STOP IT BUT I CAN ENFORCE CERTAIN POLICIES THAT WILL LIKELY PROVIDE THAT OUTCOME.

THAT OPTION DOESN'T EXIST TO ME TO MINIMIZE THE CONTEXT COLLISIONS ON THE INTERNET AND I THINK THAT'S A CONCERN.

>> ON THAT LOVELY IMAGE --
(LAUGHTER)

-- I THINK WE HAVE TO MOVE ON AND I'M GOING ASK EVERYONE'S INDULGENCE TO LET US GO FOR A FEW MINUTES BECAUSE THERE ARE A COUPLE QUESTIONS I WANT TO HIT AND THERE'S A COUPLE AUDIENCE QUESTIONS THAT COME IN AND I'LL ASK OUR PANEL MEMBERS TO REMEMBER WE ARE TIGHT FOR TIME BUT I DON'T WANT TO ASK YOU A COUPLE MORE QUESTIONS ABOUT LOOKING FORWARD A LITTLE BIT ARE COMPANIES COMPETING OVER PRIVACY AT THIS POINT?

ARE WE SEEING PRODUCTS THAT ARE OFFERING MORE CHOICES FOR

CONSUMERS ABOUT HOW MUCH OF THEIR INFORMATION THEY SHARE ONLINE?

>> WE ARE IN BROWSERS -- COMPARE CHROME'S PRACTICE TO FIREFOX OR FOR WIRELESS TEXT MESSAGES THE LET'S APP SERVICE TO THE APPLE MESSAGING OR CARRIER TEXT MESSAGING.

SO WE ARE SEEING SO WE ARE SEEING DIFFERENTIATION ON THE MARKETPLACE FOR ADVERTISING AND PRIVACY PRACTICES.

>> I THINK THERE'S NO DOUBT IT HAPPENS IN VARIOUS WAYS. THE SEARCH SPACE THERE'S A STARTUP CALLED DUCK, DUCK, DOE WHICH PROMOTES ITS WHOLE PRODUCT AS NOT RETAINING ANY INFORMATION ABOUT YOUR SEARCH QUERIES. STICKING WITH A SEARCH QUERY SPACE FOR A NUMBER OF YEARS AGO THERE WAS DEBATE ABOUT THE RETENTION OF SEARCH QUERY DATA AND YOU SAW A WAR BETWEEN A NUMBER OF SEARCH ENGINES ALONG HOW THEY WERE GOING TO COMPETE IN THAT SPACE.

WE'VE SEEN THIS IN THE BROWSER SPACE GOOD DEALING+ TRIED TO ADVERTISE THAT PRODUCT WHICH GIVES YOU MORE CHOICES THAN OTHERS.

SO NO DOUBT IT HAPPENS. THERE'S MARKETPLACE FOR THAT AND I THINK AND I THINK COMPANIES MAKE SPECIFIC MARKETING DECISIONS AND PROMOTE THOSE PRIVACY CHOICES.

>> RIGHT.

I WANTED TO THROW IN THAT WE SEE THIS IN THE "DO NOT TRAP" CONTEXT.

FIREFOX IS MENTIONED.

MICROSOFT IS ANOTHER ONE WHERE THERE HAVE BEEN SOME VERY, VERY

SIGNIFICANT INITIATIVES SO
ADVANCE THE PRIVACY LAW.
ONE OF THE -- BUT ONE OF THE
ENDURING PROBLEMS IN THIS AREA
IS BECAUSE THE TECHNOLOGY IS A
COMPLEX AND BECAUSE THE
CONSUMERS DO NOT UNDERSTAND
WHAT'S GOING ON I REALLY BELIEVE
THAT WHILE WE'RE TRYING TO
COMPETE ON PRIVACY, THE MESSAGE
DOESN'T GET THROUGH VERY WELL
BECAUSE CONSUMERS DON'T HAVE AS
MUCH OF AN APPRECIATION OF WHAT
THE IMPACTS OF A PARTICULAR
FEATURE MIGHT BE BECAUSE
SOMETIMES THE PRIVACY CONCERNS
GET OUT THERE IN SUCH A WAY THAT
THEY ARE SORT OF INDISCRIMINATE.
SO IT MAKES IT HARDER FOR
COMPANY TO STAND OUT EVEN WHEN
THEY'RE TRYING.

>> IT'S HARD TO COMPETE ON
SOMETHING PEOPLE DON'T KNOW
ABOUT.

SO IF COLLECTION IS INVISIBLE,
IT'S HARD TO DIFFERENTIATE WHERE
WE HANDLE THIS INVISIBLE STUFF
BETTER THAN THE NEXT GUY.
AND WE HAVE SEEN SOME COMPANIES
MAKE ATTEMPTS TO USE IT AS A
MARKETING.

MICROSOFT'S DONE A JOB WITH DO
NOT TRACK AS A MARKETING PLAY
BUT THAT'S SPECIFICALLY DEAN AND
THE I.E. TEAM TRYING TO LEVERAGE
THAT AS KIND OF A PRODUCT
POSITIONING PLACEMENT AND OTHER
PARTS OF THE ORGANIZATION WOULD
NEED TO COME ALONG, LIKE THEIR
AD NETWORK.

I THINK THERE'S OPPORTUNITY
THERE IS BUT IT NEEDS TO BE
COMPREHENSIVE.

WHAT'S APP IS ALSO KNOWN AS THE
MOST INSECURE APP.

FOR A LONG TIME, FOR A YEAR

WOULD ALLOW ANYONE TO ACCESS ANYONE ELSE'S FULL TEXT HISTORY. BY JUST SPOOFING THEIR PHONE NUMBER.

THERE'S BEEN A LOT OF WRITE YUPS.

SO I'M ALWAYS RELUCTANT TO --

>> AND THERE'S NO BETTER EVIDENCE CONSUMERS DON'T KNOW WHAT'S GOING ON AND WE HAD AN INTERESTING ONE-HOUR TALK FROM DAN TO START THIS DAY LONG CONFERENCE AND THE NUMBER OF QUESTIONS WE RECEIVED ABOUT WHAT IS GOING ON.

>> I MEAN, THERE ARE A WHOLE LOT OF MARKETS THAT WORK EXTREMELY WELL EVEN THOUGH CONSUMERS HAVE NO IDEA ABOUT HOW THE UNDERLYING TECHNOLOGY WORKS.

THE COMPUTER ITSELF WHERE THAT MARKET WORKS JUST FINE.

>> BUT THIS IS A MARKET WHERE THE CONSUMERS ARE INVOLVED IN A BARGAIN OVER THEIR DATA AND THE CONSUMERS DON'T UNDERSTAND WHAT DATA COLLECTION IS GOING ON AS THE VERY BASIS OF THE BARGAIN AND WHERE THAT'S HAPPENING. THAT IS NOT THAT KIND OF BARGAIN.

I DON'T NEED TO KNOW HOW AN AIRPLANE FLIES IN ORDER TO BE A PASSENGER ON AN AIRPLANE BUT IF I AM SELLING -- IF I'M BUYING A FREE SERVICE IN EXCHANGE FOR A PROFILE OF MY PERSONAL DATA, I NEED TO KNOW WHAT'S GOING ON, WHAT I'M SELLING IF IT IS, IN FACT, A SALE.

OR A TRANSACTION IN ORDER FOR THAT TO BE A FAIR AND NON-DECEPTIVE BARGAIN.

>> IF YOU THINK ABOUT COMPUTERS WHERE PEOPLE HAVE NO IDEA WHAT WAS GOING ON FOR VAST MAJORITY

OF COMPUTERS BUT SOME PEOPLE
THOUGHT THEIR GAMES RAN TOO SLOW
AND PEOPLE PUSHED VIDEO CHIPS
THAT WOULD ACCELERATE THE
PROCESSING DESIGNED SPECIFICALLY
FOR GAMES THERE'S A SMALL NUMBER
OF PEOPLE WHO KNOW ABOUT THAT.
THOSE THAT ARE INTERESTED IN
THAT ATTRIBUTE, THAT ATTRIBUTE
SPREADS.

OR THINK ANTI-LOCK BRAKES.
CONSUMERS HAVE NO IDEA HOW
ANTI-LOCK BRAKES WORK.
THEY'RE WILLING TO BUY THE
SAFETY BENEFIT.

THE PROBLEM IN THE MARKET WHEN
THESE THINGS FAIL-- IF THEY
FAIL-- AND WE DON'T KNOW YET
THAT YET, BUT IF THEY FAIL IT'S
PROBABLY BECAUSE THERE'S NOT
ENOUGH CONSUMERS WHO CARE
>> BUT WITH GRAPHICS CARDS-- AND
I WAS ONE OF THOSE CONSUMERS--
CONSUMERS CAN SEE THAT THEIR 3-D
GAMES ARE THROWING LOTS OF
TRIANGLES AND THAT THE FRAME
RATE IS HIGH.

CONSUMERS CANNOT SEE WHAT IS
GOING ON WITH THE THEIR DATA
BECAUSE IT'S OPAQUE AND THAT'S A
FUNDAMENTAL DIFFERENCE AND I
THINK HOWARD IS JUST INACCURATE
ABOUT THE ANALOGY TO THOSE KINDS
OF MARKETS.

>> I THINK A BETTER ANALOGY--
AND IT MIGHT BE A LITTLE
INAPPROPRIATE FOR THIS
AUDIENCE--
(LAUGHTER)

>> SO I'VE DECIDED I'M GOING
START A HOTEL CHAIN.
A NATIONAL HOE TILL TELL CHAIN
THAT AS TRAVELERS TO STAY FOR
FREE.
THE ONLY IS THAT THE TRAVELERS
WHO COME THROUGH MY HOTEL I HAVE

CAMERAS INSTALLED.
I BLUR OUT THEIR FACES AND
TATTOOS BUT SELL IT AS A PORN
SITE.

SO THERE'S NO HARM, THEY'RE
RECORDED, THEIR DATA IS BEING
USED BUT THEY'RE GETTING THIS
GREAT SERVICE FOR FREE AND THEY
DON'T NEED TO KNOW ABOUT IT
BECAUSE THEY GET A FREE SERVICE.
SHOULD WE --

>> ISN'T THAT A HOTEL ON THE
HIGHLINE IN NEW YORK?

>> I THINK IT ALREADY EXISTS,
IT'S NOT A HYPOTHETICAL.

(LAUGHTER)

>> IT'S STILL PRICEY, THOUGH.

>> THAT'S PRETTY CLEARLY A HARM.

>> WHY IS THAT A HARM?

>> IT'S BEEN A HARM AT TORT LAW
FOR AGES.

YOU CAN'T USE SOMEBODY'S IMAGE,
IT DOESN'T MATTER --

>> I BLOCKED OUT THEIR FACES.

>> THAT'S A HARM.

>> SO WHY CAN --

>> REASONABLE PEOPLE THINK
THAT'S A HARM.

>> WHY CAN YOU USE MY DATA WHICH
IS VERY MUCH MY LIKENESS.

>> REASONABLE PEOPLE DON'T THINK
THAT'S A HARM.

(LAUGHTER)

>> I THINK THAT'S A SUFFICIENTLY
LOADED --

>> SOME REASONABLE PEOPLE DO.
BUT THAT'S NOT A TORT BECAUSE --

>> THAT'S WHAT WE'RE HERE TO
DISCUSS.

>> BECAUSE THE LAW HAS NEVER
SEEN THAT HAS THAT AS A PROBLEM.

>> OUR PRIVATELY LAW ISN'T
LIMITED TO TORT LAW!

WE HAVE LOTS OF -- THE IDEA THAT
PRIVACY LAW IS NO DIFFERENT FROM
WARREN AND BRANDEIS WROTE ABOUT

IN 1890 IS ABSURD!

LIMITING THINGS TO TORT-SPECIFIC HARM, WE HAVE -- ARE WE GOING TO REQUIRE PHYSICAL INJURY IN ORDER TO HAVE A PRIVACY HARM? I MEAN, I THINK THE IDEA OF --

>> THAT'S PRETTY CLEARLY --

>> IT'S ONE THING FOR US TO LOOK FOR PROBLEMS, FOR DANGERS, FOR RISKS.

BUT WE DON'T LOOK FOR HARM -- WE DON'T NEED LOOK FOR HARM -- WE DON'T NEED TO LOOK FOR PHYSICAL HARM OR FRONT PAGE NEWS, THIS HORRIBLE THING HAS HAPPENED TO THIS PERSON.

AS ASHKAN SAID BEFORE, WHEN WE'RE TALKING ABOUT AGGREGATE BENEFITS, WE LOOK AT SOCIETAL BENEFITS FROM TRAFFIC SAFETY AND TRENDS.

WHY CAN'T WE LOOK TO SOCIETAL BENEFITS FROM PRIVACY?

LIKE PEOPLE ABLE TO READ FREELY AND NOT BE -- WE CAN'T MEASURE IF SOMEONE DOESN'T READ A CERTAIN KIND OF SUBVERSIVE OR POLITICAL ARTICLE BECAUSE THEY'RE AFRAID THEY'RE BEING WATCHED.

BUT IF WE'RE SHAPING OUR POLITICAL DISCOURSE, SHAPING OUR READING, THAT IN HOWARD'S TERMINOLOGY IS A HARM.

BUT I THINK MUCH MORE POINTEDLY IT'S A DANGER, IT'S A RISK.

SOMETHING WE SHOULD BE CONCERNED ABOUT.

IT IS POSSIBLY AN UNFAIR PRACTICE OR DECEPTIVE PRACTICE. THAT'S WHAT WE'RE HERE TO TALK ABOUT.

WE'RE NOT HERE TO TALK ABOUT NARROW SOLELY TORT LAW FOCUSED NOTIONS OF HARM.

PRIVACY LAW IS MUCH MORE BROAD

THAN THAT.

AND CONSUMERS' INTEREST IN THESE KINDS OF TECHNOLOGIES AND THESE KINDS OF DANGERS RATHER THAN HARMS IS MUCH MORE BROAD THAN THAT, TOO.

>> ALL RIGHT.

AND IT'S GETTING INTERESTING AND I HATE TO CUT IT OFF.

(LAUGHS)

WHY COULDN'T YOU GUYS START FIGHTING EARLIER?

(LAUGHTER)

I THINK WE'LL HAVE TO START WINDING UP A BIT BECAUSE WE ARE OFFICIALLY OVER TIME AT THIS POINT.

I WANT TO ASK ONE AUDIENCE QUESTION AND I APOLOGIZE TO EVERYONE WHOSE QUESTIONS WE WEREN'T ABLE TO GET TO BECAUSE WE HAVE A LOT TO TALK ABOUT AND I'LL ASK EACH OF YOU TO GIVE US YOUR SUM-UP THOUGHTS IN VERY LITTLE TIME.

SO IF YOU WANT TO START THINKING ABOUT THAT.

LET ME ASK YOU THE QUESTION FIRST.

WE HAD AN AUDIENCE MEMBER WHO ASKED IF -- AND THIS IS PRETTY RELEVANT TO WHAT HOWARD WAS JUST SAYING.

IF THINGS ARE CHANGING, IF THERE'S A -- IF THINGS ARE COLLECTED ARE CREATING NEW HARMS AND DANGERS MAYBE WE'RE LOOKING AT A PARADIGM SHIFT.

ARE THERE WAYS THAT CONSUMERS CAN AFFECT THIS INDIVIDUALLY AND MORE BROADLY?

SO ARE THERE THINGS THEY CAN INDIVIDUALLY DO TO PROTECT THEMSELVES AND MORE BROADLY AFFECT THE DISCUSSION AND MAKE THESE -- THEIR INTERESTS IN THIS

KNOWN?

>> WELL, CONSUMERS DO.
THE WELL-PUBLICIZED SORT OF USER
REBELLION AGAINST, SAY, FACEBOOK
CHANGES IN TERMS OF SERVICE
REFLECT A VERY HIGH LEVEL OF
SOPHISTICATION WITH A VERY LARGE
NUMBER OF USERS THAT DO PUSH
BACK AND AFFECT THE KIND OF
PRIVACY PROTECTIONS AND POLICIES
THAT ARE PROVIDED

>> I THINK IF THEY KNOW ABOUT IT
CONSUMERS WILL PUSH BACK ABOUT
-- ON THINGS THEY KNOW OR ARE
MADE AWARE OF BUT MOST PEOPLE
DON'T KNOW HOW THEIR AUTOMOBILES
FUJS AND MOST PEOPLE DON'T KNOW
IT'S POWERED BY THEIR DATA JUST
LIKE I DON'T OWN MY HOTEL.

(LAUGHTER)

>> LET ME GO AHEAD AND GIVE YOU
-- I ORIGINALLY SAID A WHOLE
MINUTE BUT WE'LL HAVE TO CUT IT
DOWN TO 30 SECONDS.
TWO SENTENCES, TELL ME YOUR
SUM-UP OF YOUR THOUGHTS.
WE'LL START WITH MIKE AND WORK
OUR WAY DOWN.

>> WELL, TO PAR PHRASE THE MOVIE
FROM A YEAR OR TWO TWO YEARS AGO
"IT'S COMPLICATED."

THERE'S NO ONE SINGLE PLACE OR
CHOKE POINT THAT WE NEED TO PAY
ATTENTION TO WE REALLY NEED TO
FOCUS ON WHAT IT IS THAT
POLICYMAKERS WANT TO ACCOMPLISH.
WHAT ARE THE HARMS THAT NEEDED
TO BE PREVENTED OR POLICED
AGAINST?

JUST AS WATER SEEKS ITS OWN
LEVEL, IF YOU TRY TO FOCUS ON
ANY DIFFERENT LAYERS IN THE
STOCK, THE CONDUCT WILL FIND ITS
TRY ANOTHER LAYER SO A BIT OF A
FOOL'S ERRAND LOOKING AT THE
LAYERS.

ENCOURAGE EVERYBODY TO LOOK AT THE HARMS OF THE PROBLEMS YOU WANT TO ADDRESS.

>> I WOULD AGREE WITH THAT. I THINK WHAT WE HAVE TO LOOK AT IS THE TAKE DANGER AND THE VALUES THAT ARE THREATENED BY THE COLLECTION OF DATA ABOUT ALL OR MOST OF YOUR ACTIVITIES ACROSS MULTIPLE PLATFORMS. I THINK WE NEED TO TALK ABOUT -- THERE'S A MASSIVE MARKET IN ALL OF OUR READING HABITS AND ALL OF OUR SEARCH QUERIES. AND I THINK WE NEED TO WORRY ABOUT THAT.

WE NEED TO WORRY ABOUT NOT JUST INTELLECTUAL PRIVACY BUT ALSO ABOUT THE POWER IMBALANCES WITH CONSUMERS WHEN THEY'RE OFFERED IN MULTIPLE PLATFORMS AND TIMES AND ALSO AT THE LURKING THREAT THERE IS A POTENTIAL TO GOVERNMENT ACCESS TO THESE MASSIVE HIGHLY DETAILED HIGHLY SENSITIVE DATABASES.

>> I THINK WE'LL LOOK BACK AT THIS AND FIND IT RIDICULOUS THAT WE WERE AT THIS POINT IN TIME THE SAME WAY WE LOOK BACK AT COUNTRIES OR COMPANIES BEING ABLE TO GO INTO CERTAIN NATURE RESERVES AND EXTRACT THE RESOURCES WITH NO RECOURSE. THERE'S AN OPPORTUNITY TO DEMONSTRATE THAT THERE IS A GREAT DEAL OF VALUE ON THIS INFORMATION BUT THIS INFORMATION IS CO-OWNED BETWEEN THE PEOPLE THAT GENERATE IT AND PEOPLE THAT COLLECTED AND DATA MINE IT AND I THINK ALONG THESE LINE THERE IS'S OPPORTUNITIES TO DO BETTER IN TERMS OF PROVIDING HIGH QUALITY DATA THAT CONSUMERS KNOWINGLY AND WILLINGLY ENGAGE

AND LEAVING INFORMATION THAT THEY FIND SENSITIVE OR DON'T WANT TO PARTICIPATE IN THIS MARKETPLACE OFF THE TABLE.

>> THE COMMISSION AND THE PRIVACY REGULATION EFFORT IN PARTICULAR SHOULD FOCUS ON INFORMATION AND ITS USES. IT SHOULD DO THAT IN ORDER TO SEEK TO AVOID BAD CONSEQUENCES FOR CONSUMERS.

THAT DOESN'T MEAN AS I THINK I PRETTY CLEARLY SAID NARROWLY PHYSICAL OR ECONOMIC HARM. IT INCLUDES A LOT OF REPUTATION KINDS OF HARMS AS WELL.

BUT IF YOU CAN'T ARTICULATE WHAT THE HARM IS YOU CANNOT PREVENT IT.

IF THE ONLY HARM THAT WE'RE WORRIED ABOUT IS SPECULATIVE POSSIBILITIES OF WHAT MIGHT HAPPEN AT SOME POINT IN THE FUTURE, THERE'S ALWAYS GOING TO BE SPECULATIVE POSSIBILITIES OF WHAT MIGHT HAPPEN AT SOME POINT IN THE FUTURE AND WHAT WE'RE LIKELY TO DO IS PRECLUDE A LOT OF REALLY USEFUL SERVICES ON THE HORIZON THAT NONE OF US HAVE EVER THOUGHT OF YET.

>> I AGREE WE THIS STATEMENT THAT WE SHOULD WORRY ABOUT THE DIFFERENT IMPLICATIONS IN THIS DEBATE AND I THINK THAT'S WHY FORUM IS GOOD.

THERE'S OTHER FORUMS THAT -- THE FUTURE OF PRIVACY FORUM, PEOPLE ARE DOING A LOT OF THINKING ABOUT THIS.

THE QUESTIONS ARE THE SAME QUESTIONS WE'VE BEEN ASKING FOR A LONG AS PEOPLE HAVE BEEN COLLECTING INFORMATION. IT'S HARD TO COME UP WITH COMPREHENSIVE SPECIFIC YOU HAVE

TO DEFAULT INTO WHAT ARE THE USES OF DATA AND THE HARMS IN ORDER TO IN ORDER TO PREVENT THE COLLATERAL PROBLEMS OF OVERREGULATING AND TREATING UNINTENDED CONSEQUENCES THAT INVOLVE THE HARM AND THE FREE FLOW OF INFORMATION.

THANK YOU.

>> I THINK THAT -- I AGREE WITH ASHKAN AND NEIL ESPECIALLY, BUT THE THING THAT -- THE WORD THAT I WANT TO EMPHASIZE IS FAIRNESS, OR UNFAIRNESS.

BECAUSE I THINK THAT WE HAVE TO -- WE ARE SEEING TWO VERY, VERY DIFFERENT LEVELS AT WHICH THERE IS A FAIRNESS PROBLEM.

THE FIRST IS SIMPLY AT THE EXTRACTION COLLECTION OR SORT OF INDUCEMENT ABOUT AND FROM CONSUMERS WITHOUT ANY KNOWLEDGE OR UNDERSTANDING OF WHAT -- WHO IS COLLECTING IT, WHAT IS BEING COLLECTED AND WHAT IS BEING USED FOR THEN YOU HAVE TO FAIRNESS PROBLEM SURROUNDING USES.

THERE HAVE BEEN GREAT STORIES IN THE LAST COUPLE OF MONTHS ABOUT CREDIT SCORES AND E-SCORING AND ALL OF THE DIFFERENT WAYS THAT PEOPLE ARE BEING JUDGED AND DECISIONS ARE BEING MADE ABOUT THEM BASED ON THIS KIND OF INFORMATION AND ALSO BASED ON ALGORITHMS OR MEANS OR SCORING FOR WHICH THE CRY TIER WAR ARE COMPLETELY UNTRANSPARENT SO YOU HAVE ON THE ONE HAND THE INPUT SIDE OF THE DATA AND ON THE OTHER YOU HAVE TO JUDGMENT SIDE ABOUT THEM AND THERE ARE SIGNIFICANT QUESTIONS OF FAIRNESS THAT ARE TIED TO PRIVACY BUT ARE DISTINCT FROM PRIVACY FOR BOTH OF THOSE

PROCESSES.