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

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 SUGENANd ( )Tj H.004 T EMC </MCID10(L)ASE>>B5-16.01 -1U

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 TH.

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

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.

>> 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 O4(T)-6j EMC O13d ( )T Tc 0 Tw 13.HING B34 -1.15 Td [(A SO273.15

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, GOVERNMENTES CAN USE TECHNOLOGIES TOO.
EVEN IF WE'RE NOT CONCERNED ABOUT DIRECT GOVERNMENT SURVEILLANCE THE CREATION OF THE DATABASES, INTELLECTUAL PROFILES, HIGHLY GRAN AOU HRAR CONSUMER PROFILES TO PREDICT INDIVIDUAL BEHAVIOR AND LEARN ABOUT INDIVIDUAL IDENTIFIABLE PEOPLE IS SOMETHING TKPOFT COULD BE PARTICULARLY INTERESTED IN EITHER AS A MARKET PAR ADVERTISE PAPT, 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 A 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'TORMAT29 N( )Tj EMC c 0 Tw115' Tc A6(H)5LIDT BEAR Tw - IDTHILI
>T(O)11(O)1(K AN)5(T(O)-4(RM)]TJ 0 Tc 0 Tw 19.5640 Td ( )Tj EMC /P <</MCID 326C 0.003 Tc -0

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

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

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.

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 OPERAT OPERAAT O2 OPERAA(F)4(F)4(ER)5(EN)15(T)-6(O)11(1)-11(').0

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

0 Tc 0 Tw 14.06 0Td ( )Tj EM

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.

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'SSACAJ 0 A29PN Tc 0 TN-1(Q5j EO)16(W)-38(Y10(H)Td ( )Tj E(W)-3CEKO)1(MF0(N)F0(N)1)T

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

THROUGH V.P.N. OR APPS IN
DIFFERENT PATHS THAN INTENDED SO

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.

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 TWITER

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

WHAT ABOUT
THE U.S.?

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

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

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

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.

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
QUEST ES-3V-10(C34(NG)-4(US)-5(E)-5(D F)-1(O)-0R)5(KE)10(T)-6(I)1(N)5(G)1( )>BDC(T)-6(BDC

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

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.

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 FAR
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 VERYTJ 0 d [((E V)106(H)15(E)0 Tc 033(E)10(G/E V)10(0 Td (B5(RS)-5( )-f /E V)10(06(H)145)S

QNGMTB5(RS)-5( )-f /E V06(H)140 Td ( )Tj EMC /P <</MCID 172 Tw -A/P <</M

MMLVEAT

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

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
>> AE AT T

)6<(RA)-

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 PROVIDEED
>> I THINK IF THEY KNOW ABOUT IT CONSUMERS WILL PUSH BACK ABOUT
-- ON THINGS THEY KNOW OR ARE

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 THOUS THATOHDI TTAT

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

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
CET Tw8.B HARMU <</MCID 11 >>BDCI>> I THIAL D3 Tc (--)Tj Td (-w [(CRE)5) Td (Tw 8.00 TdD

PROCESSES.