

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

HOUSE JUDICIARY COMMITTEE
PUBLIC HEARING ON HB 2590
JEFFERSON HILLS MUNICIPAL CENTER
925 OLD CLAIRTON ROAD
JEFFERSON HILLS, PA 15025

Majority Chairman Ron Marsico
Representative Rick Saccone
Representative Bryan Ellis
ALSO APPEARING:
Michael Kane, Legal Counsel
Lauren Orazi, for Minority Chair Caltgirone

September 18, 2012

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

INDEX

Dave Freed	9
George H. Pike	26
Major Marshall Martin	44
Corporal John O'Neil	44
Mr. A. Sheldon Kovach	51

1 CHAIRMAN MARSICO: Good morning everyone. Can
2 you hear me okay? Thank you. I'm Representative Ron
3 Marsico, the Chair of the House Judiciary Committee.

4 I would like to welcome everyone here and also
5 thank Jefferson Borough for your hospitality hosting us
6 here today for this very important bill we are going to
7 discuss, House Bill 2590 introduced by Representative Rick
8 Saccone. Representative Saccone is here and will make
9 comments, remarks after I finish mine.

10 House Bill 2590 is an important piece of
11 legislation that will greatly help law enforcement
12 identify individuals who use the internet to sexually
13 abuse and exploit children. It will give the Attorney
14 General and the District Attorney the authority to issue
15 administrative subpoenas to get basic subscriber or
16 customer ID, identification information from that source
17 service provider or the person using the services to
18 exploit or abuse children.

19 Today a lengthy process is necessary to get a
20 Court Order for information which our Supreme Court said
21 is not private. Because time is of essence in many of
22 these cases, the ability to use a subpoena will greatly
23 speed up the process, enhance the law enforcement's
24 ability to investigate the crime and protect children.

25 I want to thank Representative Saccone for his

1 work in introducing this piece of legislation and his hard
2 work actually for the last almost two years on the
3 committee.

4 We have several witnesses today who will share
5 their thoughts and give us information. We will start
6 with District Attorney Dave Freed. But before we bring up
7 D.A. Freed, I will ask Representative Saccone to give a
8 few remarks.

9 REPRESENTATIVE SACCONI: Thank you
10 Mr. Chairman, thanks for holding this hearing in my
11 district and thank the testifiers for coming a long way to
12 participate. I know some of my colleagues are still on
13 their way coming the rain has held them up and I thank
14 everyone who has come along way to be here and
15 participate.

16 I do think it is important that we bring
17 Harrisburg out to the people. We try to do this on the
18 Judiciary Committee a lot so government doesn't seem so
19 distant. People tell me all the time everything that goes
20 on in Harrisburg they don't pay attention. We love to see
21 it when we bring the government to them. That is what we
22 are doing here today.

23 We do have a troubling problem in America today
24 with pornography. It is a sickness slowly absorbing more
25 people in our society at a younger age than ever before.

1 I want to share a couple statistics with you. According
2 to the Family Safe Media there are 4.2 million
3 pornographic Websites on the internet, 12 percent of all
4 Websites. Over 420 million foreign pages pornographic web
5 pages. About 25 percent of the daily search engine
6 requests are related to porn. 34 percent of internet
7 users report unwanted exposure porn on the web. The most
8 troubling is child pornography.

9 There are over 100,000 Websites offering
10 illegal child porn. 89 percent of our youth report some
11 kind much sexual solicitation in chat rooms. One in seven
12 youth have received some type of sexual solicitation
13 on-line. The average age of first internet exposure to
14 porn is 11 years old.

15 90 percent of our youth eight to 16 report
16 having viewed porn on-line, most while doing their
17 homework. And the largest consumer of internet porn is at
18 the age group of 35 to 49, the ones out there either
19 watching or trying to take part in this.

20 The top producers porn in the world are the USA
21 and Brazil. So I think it is our duty to protect children
22 from those who would spoil their childhood through sexual
23 exploitation. We need tougher laws to go after those who
24 prey on our children and that's why part of why we are
25 here today and I'm happy to be part of the effort to crack

1 down on this blight on our society. So I thank you all
2 for coming. Thank you, Mr. Chairman.

3 CHAIRMAN MARSICO: We will have counsel Mike
4 Cane give a brief explanation of the Bill then call up
5 District Attorney Freed.

6 MR. KANE: Thank you Mr. Chairman. Just by way
7 of background with the emergence of the internet a lot of
8 information obviously is stored on servers that are owned
9 by third party internet service providers and
10 communications providers. That is a lot of information
11 about a lot of people so Congress passed to protect the
12 privacy of individuals, passed what is called the Stored
13 Communications Act which is Title 18, United States Code,
14 Section 2703.

15 Section 2703 provides a framework for getting
16 information from these service providers, particularly by
17 the government having access to this information. It
18 includes sections that govern acquisition of content likes
19 e-mails and those sort of things and also non-content
20 information. And provides for various mechanisms using
21 subpoenas or search warrants to get that information.

22 One of the sections of the Federal FSCA Section
23 2703(c)(2) that allows, provides that if Congress so
24 authorizes, information that is basic identification
25 information, name, address, local and long distance

1 telephone, not the numbers called, but the local long
2 distance telephone records about when calls were made, the
3 length and types of service, the telephone and instrument
4 number, the IP address of a computer that was used. All
5 these things can be gotten if an administrative subpoena
6 is used authorized by either state or federal law.

7 The United States has, Congress has authorized
8 the use of a subpoena in another section of the Federal
9 Crimes Code Section 3486. And that provides that the
10 United States Attorney General may utilize an
11 administrative subpoena to get basic information in
12 connection with an investigation of child sexual
13 exploitation or child sexual abuse. The information is
14 limited to those things that I talked about before about
15 name and address.

16 Pennsylvania has adopted its own Stored
17 Communications Act, that is at 18 Pennsylvania
18 Consolidated Statute Section 5743.

19 It essentially mirrors the federal act and also
20 says that if a validly authorized administrative subpoena
21 is used that basic subscriber information can be gotten as
22 well. Pennsylvania though has never enacted a statute to
23 permit the use of administrative subpoena unlike the
24 federal statute.

25 House Bill 2590 does that. It would allow the

1 Attorney General or a District Attorney to issue an
2 administrative subpoena to an internet service provider or
3 someone that is storing information about a customer or a
4 subscriber only though to get the name of the person, the
5 address of the person, the telephone number of the person,
6 the IP address that was used on a computer that that
7 person subscribes to through the service. And by enacting
8 House Bill 2590 not only would we give Pennsylvania
9 authority under our Stored Communications Act, it would
10 also meet the requirements of the federal Stored
11 Communications Act for use of an administrative subpoena
12 which will greatly assist law enforcement in identifying
13 those who use the internet to perpetrate these kinds of
14 crimes against children.

15 CHAIRMAN MARSICO: Thank you, Counsel Kane.
16 One update. Introduce yourself down this way.

17 REPRESENTATIVE ELLIS: Good morning. Brian
18 Ellis from the 11th District in Butler County. Sorry I'm
19 late.

20 MS. ORAZI: Laura Orazi.

21 CHAIRMAN MARSICO: Thank you very much, good to
22 see you and thanks for being here. We made some opening
23 statements. Our first testifier like I said before
24 starting out is Dave Freed, the District Attorney from
25 Cumberland County who is also the Vice President of the PA

1 DA'S association. Welcome and you may proceed.

2 MR. FREED: Thank you, good morning. Thank you
3 for the invitation to PDAA and the opportunity for us to
4 provide comment on this bill. I'd say good morning to
5 Chairman Caltgirone but he has been replaced by a much
6 more pleasant person so it is wonderful to have her here
7 today.

8 And Representative Saccone, good morning nice
9 to be in your territory and Representative Ellis, good
10 morning to you as well.

11 My name is David Freed and I'm the District
12 Attorney of Cumberland County and I'm also the Vice
13 President of the Pennsylvania District Attorney's
14 Association. I'm here today to speak about the merits of
15 House Bill 2590.

16 This is an era of incredible technological
17 advances and countless ways technology aids and improves
18 our lives every day. But the unfortunate reality is that
19 as technology becomes more sophisticated so too are the
20 ways that it is misused and exploited.

21 Today cyber crimes are more prevalent and more
22 varied than ever. Criminals routinely use or rather
23 misuse technology to commit crimes ranging from economic
24 fraud, cyber bullying and of course the trafficking and
25 sharing of child pornography and the creation of it

1 Representative Saccone alluded to in his remarks. And
2 certainly that is the most alarming portion of what we are
3 dealing with.

4 For the safety and well-being of our children
5 these crimes must be stopped. This important piece of
6 legislation assists us in that endeavor by helping us to
7 stay a step ahead of the criminals.

8 I think it is particularly appropriate to have
9 a District Attorney here and State Police and the
10 Representative from Delaware County where the Internet
11 Crimes Against Children Task Force is housed. We all as
12 District Attorneys end up doing a lot of these cases and
13 that is actually the model for the case often for us in
14 Cumberland County is we get a tip from the Internet Crimes
15 Against Children Task Force. We start the investigation
16 and then when we go to actually put boots on the ground
17 and hit the streets we have assistance from our friends in
18 the State Police so it is a group that works pretty
19 seamlessly together. In order to successfully investigate
20 these cases we have to rely on the cooperation of
21 electronic communication providers. They are the ones
22 that have the information including internet service
23 providers. They can provide us valuable information such
24 as user's name, address, telephone number, method of
25 payment, and records relating to session times and

1 durations.

2 When criminal activity is suspected, this
3 identifying information is a vital tool for law
4 enforcement. Without it we not be able to locate the
5 source of the crime.

6 I will give you a quick example the way a
7 typical child pornography dissemination or possession case
8 might come to the attention of the District Attorney. The
9 Internet Crimes Against Children Task Force of Delaware
10 County have people that are constantly monitoring the
11 internet for sharing of child pornography. If they see a
12 sharing going on, they send a tip to people they train in
13 the area. Once that tip is received, the investigators
14 check out the tip and they see that yes, there is sharing
15 going on where someone has software configured to allow
16 the sharing. And then they can do proactive steps to see
17 if they actually will share child pornography.

18 Once that happens, we know that there is
19 somebody on the other end essentially of a line or a
20 wireless connection and sharing, we need to figure out who
21 that is. In order to do that, we look at the unique IP
22 address then we have to go to the company that houses that
23 address for that identifying information.

24 Right now the way that we need to do that
25 generally is with a search warrant or a Grand Jury

1 subpoena. That is a process that we can do, need probable
2 cause for a search warrant, certainly need probable cause
3 to establish grounds for a Grand Jury investigation.

4 While the law allows us to use a Court Order to
5 do this, there is no process in place to obtain the Court
6 Order and to lay out the requirements for the Court Order.
7 That is what this statute does. So it simplifies and
8 speeds up that process, allows us to stay one step ahead.

9 Search providers are generally responsive to
10 us. We work with them on a regular basis. They provide
11 valuable assistance to us. But obtaining that information
12 is not without challenges and there are instances that
13 some service providers don't want to cooperate or don't
14 give a timely response.

15 Noncompliance is a serious concern for all of
16 us and threatens to compromise criminal investigations.
17 When investigations break down, the criminal activity may
18 continue unchecked and additional harm may be done to
19 victims.

20 This is not to cast aspersions against service
21 providers or highlight the consequences when we meet
22 resistance. As I said, our present option is a search
23 warrant and many of the service providers are located
24 outside the state, frequently based in California.

25 I was talking with the State Police reps out in

1 the hall, for a long time we had a company in California
2 that say we need a search warrant so we have to try to
3 figure out a way to get a search warrant in California.

4 AOL for a time there was when they were based
5 in Northern Virginia, there was a group in that police
6 station in Northern Virginia you call that would help you
7 with search warrants. But it was not a simple process.

8 The legislation that is in front of you
9 squarely addresses the problem because it provides for
10 administrative subpoenas. An administrative subpoena
11 doesn't require probable cause, doesn't require approval
12 by a court but in contrast to a search warrant, it is a
13 Court Order.

14 If a service provider doesn't want to comply
15 with the subpoena, they bare the burden of explaining why
16 to the court. Otherwise, the subpoena can be enforced
17 through the courts and local jurisdiction which is very
18 important. If internet service providers are doing
19 business in our jurisdiction, we can bring them into court
20 and have them explain noncompliance rather than going to
21 California, Virginia or somewhere else to try to get this
22 information.

23 With the assistance of our courts, the records
24 custodian for the company can be compelled to appear in
25 Pennsylvania court with requested information.

1 As I mentioned a moment ago, historically there
2 are differences in the companies about what they require
3 depending on what their compliance people tell them,
4 whether they want a search warrant or Court Order. A
5 search warrant we in law enforcement know how to do that.
6 But a Court Order we used to say well this is a subpoena
7 Court Order, a Grand Jury subpoena of a Court Order.
8 There is no process in place that is used to frustrate me
9 greatly, still does sometimes when somebody says we need a
10 Court Order when there is no legislative mechanism or rule
11 for us to go get a Court Order.

12 This cures that problem entirely. There is a
13 process to get a Court Order we can hand the Court Order
14 to the company and they provide us the information.

15 So where a search warrant falls short, subpoena
16 is an effective remedy. Subpoena power will have an
17 immediate and direct impact on our ability to stop cyber
18 crime at the source.

19 Finally, it is important to note this
20 legislation is constitutionally sound insofar as it is
21 limited in the information it covers. It allows access to
22 specific records concerning identity of the subscriber.
23 It does not allow access to content which would still
24 require a prior showing of probable cause and prior
25 judicial approval.

1 In the example I gave earlier of a tip and then
2 attempt to figure out who we are dealing with, once we
3 have that information and we know that their software is
4 configured to share child pornography or have shared child
5 pornography, then we have probable cause, then we get a
6 search warrant, then we can get the content information.

7 So the administrative subpoena just allows us
8 to find out the identity which is one step in building
9 probable cause. It doesn't automatically equate to
10 probable cause but it is an important step. In this way
11 it strikes an appropriate balance in the interest of law
12 enforcement versus privacy rights of individuals. It is
13 limited and targeted not intended to cover contents of
14 communication. I think councilman Kane mentioned this but
15 I will highlight in the bill specifically it allows us to
16 access subscriber customer's name, address, telephone
17 number or instrument number or other subscriber number
18 identity including any temporarily assigned network and
19 address.

20 HB 2590 addresses a serious hurdle to
21 confronting cyber crime, especially predatory attempts
22 against children. In doing so it not only assist law
23 enforcement but helps to protect citizens of the
24 Commonwealth from growing threat. I want to be very clear
25 that while I have given examples the way things are done

1 in Cumberland County, this is an issue across the state,
2 it's been an issue of much discussion within the District
3 Attorney's Association. And there is strong support from
4 our membership for this bill. It is a common sense bill
5 that allows us to use a tool that has been provided by the
6 Legislature and gives us a mechanism to get the
7 information. And this is vital information.

8 Most of the time it is going to help us ferret
9 out people that are sharing and disseminating child
10 pornography, but think of the case where we see
11 information and it appears that it is showing ongoing
12 actual child abuse. There are cases of actual child abuse
13 that have been broken using this method. So while it is
14 important for us, frankly more of the cases we do are
15 possession and dissemination, this is also the first step
16 in actually protecting the kids who are the subject of
17 these images. It is very important to remember.

18 I want to thank the Committee for the
19 opportunity to present and again thank Representative
20 Saccone for hosting us in this beautiful building and
21 introducing this bill. I'm happy to answer any questions
22 anybody has.

23 CHAIRMAN MARSICO: Thank you, Dave, any
24 questions of staff, members? Representative Ellis.

25 REPRESENTATIVE ELLIS: Thank you, Dave, for

1 being here today. I just have a couple questions. An
2 administrative subpoena so I understand that correctly,
3 can you go over again the difference between a regular
4 subpoena and an administrative subpoena and maybe have
5 examples of the way you guys use administrative subpoenas
6 now?

7 MR. FREED: Yes, a subpoena that is issued
8 through the court is done generally upon request and
9 issues through the Clerk of Courts office. An
10 administrative subpoena by contrast comes from the
11 prosecutor. And if we have a case open, criminal
12 investigation open now, we can issue subpoenas through
13 that case for records. A subpoena through the court.

14 What an administrative subpoena does is it is
15 before we have a case open in court that has been through
16 a district judge and a court doesn't have a docket number.
17 The administrative subpoena is a tool for the prosecutor
18 to use to get this identifying information. So it
19 requires less of a showing than a search warrant and it
20 relies on the discretion of the Attorney General and his
21 designee or her designee and the DA and his or her
22 designee to get information based on need. Very similar
23 in practice to a one-party consensual wiretap where the,
24 although different in the information that you seek the
25 process is that the DA authorizes it as opposed to a court

1 authorizing it. But if the subject doesn't comply, then
2 we can go into court to enforce the subpoena.

3 REPRESENTATIVE ELLIS: Well, I guess what I'm
4 wondering is about a year and a half ago I had received
5 harassing e-mails personally, very disturbing e-mails from
6 a constituent, a false name listed on the e-mail, IP
7 address. I turned it over to our legal counsel and they
8 contacted Butler County District Attorney and they
9 eventually found out who the gentleman was.

10 Would you say at that point they had to go
11 through a process that if this bill is passed would have
12 been a lot faster?

13 MR. FREED: Yes, this would greatly simplify
14 that process.

15 REPRESENTATIVE ELLIS: All they would have done
16 is --

17 MR. FREED: They would issue an administrative
18 subpoena to the service provider who would identify who
19 the person was actually attached to that address, and
20 identify the person quicker. Then ultimately they have to
21 go with a search warrant to get the information they got
22 but it would greatly speed up and simplify the process of
23 identifying the source of those e-mails.

24 REPRESENTATIVE ELLIS: Just to put it in
25 perspective, about how many times do you think in the year

1 just specifically your county this would have been?

2 MR. FREED: In my county where we are pretty
3 active on doing these kind of cases, I would say between
4 150 and 200 investigations.

5 REPRESENTATIVE ELLIS: Multiply that by 67
6 counties?

7 MR. FREED: Yes, it is a lot.

8 REPRESENTATIVE ELLIS: Thank you very much for
9 your testimony.

10 MR. FREED: Thank you.

11 CHAIRMAN MARSICO: Representative Saccone.

12 REPRESENTATIVE SACCONI: Yes, sir, thank you
13 for your testimony. Can you hear me better now? Thank
14 you for your testimony. I want to ask you this question.
15 It seems to me that these child pornographers and people
16 sharing child pornography function in cyber anonymity out
17 there and they are using the internet, the fact that they
18 can, they think their address is secret to hide behind
19 that.

20 Now, am I wrong in thinking that your IP
21 address, and I use the analogy like your house address, I
22 mean, it just tells where you live and who you are. Like
23 it is for your house, it is public information. So it is
24 no different than if you take the house number off your
25 house you think your secret, you can still find out your,

1 where you live and your address because it is public
2 information. All we are doing is making your IP address
3 and other identifying data about you public because it is
4 a public entity, public information.

5 MR. FREED: The IP addresses are unique. And
6 can specifically help to locate people. And every person
7 who signs up for an internet service, most people probably
8 don't read all the fine print. But the fine print
9 indicates that, you know, this is information that they
10 are going to hold on to and upon proper request from
11 courts they will provide that information.

12 So, there is nothing secret on the internet.
13 And although sometimes we have to jump through some hoops,
14 we can find the information that we need. This just
15 allows us to more simply access the information that is
16 held by these internet service providers while not giving
17 access to content. So, if there would be a mistake, you
18 would quickly find out when you identify the person and
19 you can't provide probable cause or probable cause shows
20 that there is not any incriminating information on the
21 system. For example, you will have an IP address come
22 back to a house where there is maybe a father, a mother,
23 use my house for example, two 42-year-olds, an
24 11-year-old, a 9-year-old and a 6-year-old.

25 Then you determine as part of your

1 investigation within that unit who is the person who
2 signed up for the IP address and who is the person more
3 likely to be using it. And those are the kind of
4 investigative things that we have to do. All it provides
5 is the address that is using it and the person who signed
6 up for it.

7 REPRESENTATIVE SACCONI: Thank you.

8 MR. KANE: Just one question, you talked about
9 child pornography cases, sharing files, can this be used,
10 for example, someone is on-line who is attempting to talk
11 a young boy or a young girl into meeting with them where
12 something is happening in realtime?

13 MR. FREED: Absolutely. And I think back to a
14 case I was again when law enforcement get together we tell
15 war stories. I was telling a war story out in the hall
16 about a case that I tried about a dozen years ago and we
17 called them traveler cases. They are cases where the
18 chats are going on then we in law enforcement arrange for
19 the offender to travel to a different place to engage in a
20 sexual liaison and arrest the person. The Attorney
21 General does a ton of those cases, Delaware County does a
22 lot of them.

23 It took us a while, it came to us through
24 internet chats, direct chats and this is back with I think
25 Yahoo Messenger back then. But this process would allow

1 us to immediately identify who the person is who is
2 engaging in that chat and the goal of this defendant was
3 to engage in this relationship with as many young people
4 as he could.

5 So, for us to be able to stop it while it is
6 going on is something even more important than images.
7 Images are the basic thing that happens most often. But
8 the traveler cases and actual abuse cases happen very
9 often and again this will speed up and assist us in being
10 able to do those cases.

11 CHAIRMAN MARSICO: Once again, you mentioned, I
12 think you mentioned how many cases you have in your
13 county. How many did you say?

14 MR. FREED: I said in terms of, if you add up
15 the potential abuse cases, the possession pornography
16 cases and other cases we would be able to utilize this
17 process I would say 150 to 200 investigations.

18 CHAIRMAN MARSICO: Any questions?

19 MR. KANE: One more question. What is the
20 relative time it takes to prepare a search warrant for
21 someone in your office, drafted, to find a judge, to get
22 it signed get it delivered as opposed to issuing an
23 administrative subpoena on those 200 cases.

24 MR. FREED: I would say the search warrant is
25 probably most of a workday with everything included, and

1 an administrative subpoena would be approval by a
2 supervisor, ask a staff person and it would take an hour.
3 The key, I think it might be in Delaware County's
4 testimony, but one more key to remember in these cases we
5 are only limited by time and resources. We could do these
6 cases all day long every day.

7 We also have rapes, robbery, murders and
8 everything else that comes before us. Anything that
9 speeds up makes and make this more simple is a huge boom
10 for law enforcement. Thank you.

11 REPRESENTATIVE SACCONI: This may not be a good
12 question for you but maybe for the computer expert. We do
13 have a question that there is a concern about what about a
14 lot of this pornography comes from overseas, will this
15 help us identify providers that are outside the country?

16 MR. FREED: Yes, all these investigations, it
17 is interesting because there is somewhat as predicted,
18 these gentlemen might be better than me to talk about
19 this, there is sometimes a limited universe of images. I
20 mean if you do this work for any length of time, you see
21 the same images over and over. Yes, certainly, anything
22 that helps us identify the source would be a positive and
23 often in our world we are sending that information on to
24 federal authorities, sending that information -- Homeland
25 Security is doing a lot of work in this area. We have

1 relationships with those groups that we can provide this
2 information and say look, this looks like an overseas deal
3 and we can provide that and share that information.

4 CHAIRMAN MARSICO: Dave, thanks a lot for your
5 time and your expertise in coming out here, we appreciate
6 it very much as always, you are always very helpful with
7 our committee and the DA's have been very, very supportive
8 in a lot of measures we deal with.

9 MR. FREED: We are strongly behind the bill and
10 appreciate the opportunity to testify.

11 CHAIRMAN MARSICO: Thanks again. Next on the
12 agenda is George Pike, professor at the, is Assistant
13 Professor of law and director of Barco Law Library,
14 University of Pittsburgh School of Law. Welcome George,
15 you may begin.

16 MR. PIKE: Thank you Representative Marsico,
17 other members of the committee. I certainly appreciate
18 the opportunity to testify before you today.

19 My written material has my background. I am an
20 Assistant Professor of Law. I teach information privacy
21 law at the University of Pittsburgh School of Law.

22 I also am a parent myself with two school aged
23 children. They are well within the demographic that
24 Representative Saccone mentioned earlier. So I need to
25 preface my remarks to any extent that it may seem like I'm

1 defending the kinds of activities that you alluded to, I
2 am absolutely not.

3 I do have some concerns about some of the
4 privacy issues being raised by this but in no way, shape
5 or form do I defend those activities. They are absolutely
6 heinous, I can recall an incident earlier in my career
7 when my children were younger I had some questions about
8 internet filtering in libraries. As an academic I had
9 those concerns. As a parent when my child typed in a
10 misspelled Disney, D-I-N-S-E-Y and encountered some
11 pornographic sites, I was very pleased that those filters
12 were in place. So I will be talking briefly about privacy
13 law and how it applies to this proposed bill.

14 Privacy law is a challenge, no question about
15 that. There is no specific privacy act out there.

16 The Supreme Court found privacy in several
17 circumstances by looking collectively at several pieces of
18 the Constitution. But there was no specific privacy act,
19 privacy constitutional right established.

20 There are privacy torts that govern the actions
21 between individuals and what information they can exchange
22 without violating the privacy of the other. And there are
23 specific privacy laws including the Electronic
24 Communications Privacy Act of which the Stores
25 Communications Act which has already been mentioned is a

1 part of that act.

2 Now this proposal implicates specifically the
3 Fourth Amendment to the Constitution which provides that
4 the right of people to be secure in their persons, houses,
5 papers and effects against unreasonable searches and
6 seizure shall not be violated.

7 From a privacy law perspective that raises an
8 interesting question because the amendment addresses
9 unreasonable search and seizures thereby creating
10 implications that certain searches are reasonable and can
11 be conducted without violating the Fourth Amendment,
12 specifically without requiring a search warrant.

13 And there is a test for determining where that
14 line applies. And we identify it as the Katz test from a
15 U.S. Supreme Court decision in 1967. And it indicated
16 that if a person has a reasonable expectation of privacy
17 and the person's house, papers and effects being seized,
18 then the Fourth Amendment is implicated and the material
19 may only be seized upon the issuance of a warrant
20 supported by probable cause.

21 If the person does not have that reasonable
22 expectation of privacy, then no warrant is required. Now
23 the test has two parts to it. The person must exhibit an
24 actual subjective test expectation of privacy. They must
25 indicate by their actions, not merely by their objective

1 statements but by their actions that they expect this
2 information, this material houses, papers, and effects be
3 considered private. Plus it must be an expectation that
4 society as a whole is prepared to acknowledge and accepts
5 as reasonable.

6 Now, the Katz test has been applied in a number
7 of circumstances and I will focus on circumstances similar
8 to what we are talking about today.

9 They do include things like pen registers to
10 obtain telephone information, the number called from and
11 the number called to were held to be outside the
12 requirement for a search warrant. It was not a reasonable
13 expectation of privacy because the phone company knows
14 that information.

15 Essentially in a nutshell if somebody else
16 knows that information even in the course of doing
17 business with that company, then you don't necessarily
18 have that expectation of privacy, it has been communicated
19 to a third party.

20 And in applying these considerations for this
21 proposed legislation, counsel mentioned the Stored
22 Communications Act and absolutely the Stored
23 Communications Act provides that a certain type of
24 information including name, address, contact information,
25 telephone connection records, length of service, telephone

1 and instrument number including temporarily assigned
2 network address is accessible under an administrative
3 subpoena such as we are talking about today.

4 And thinking about the hypothetical, I will
5 move off the prepared remarks, thinking about the
6 hypothetical that Mr. Freed provided earlier about a
7 scenario where they obtain a tip that a person is engaged
8 in exploitive behavior towards a young person, towards my
9 son, towards his son and the information being sought is
10 that that contact information, I do not believe that there
11 is a Constitutional problem, that there is a privacy law
12 problem that that scenario is completely within the Stored
13 Communications Act and to the extent the Stored
14 Communications Act is modeled by this legislation that
15 does not present in my view any kind of Constitutional
16 problem at all or any kind of privacy related problem.

17 The issue, the concern I have is privacy law
18 creates a distinction between what we call envelope
19 information and content information. Mr. Freed talked
20 extensively about content information and how this law
21 does not, this proposed legislation does not seek out
22 content information.

23 Envelope information, think about what is on
24 the outside of the envelope you mail from your house to,
25 you know, the billing company or your friend across the

1 country. It contains your address, the other address, and
2 it is seen by the Postal Service, seen by plenty of folks.
3 Content -- envelope information context of phone calls and
4 phone numbers.

5 The content information is that which is
6 contained within those envelopes, within the phone
7 conversation itself, the contents of the letter and in
8 those circumstances there clearly is an expectation of
9 privacy in that information. And content information
10 generally does require a search warrant to obtain.

11 Now the challenge is with internet content.
12 Internet information in that there is often a merger of
13 envelope and content information. For example, a URL, a
14 web address. A web address looks like envelope
15 information, looks like just simply the name, the location
16 for the web address. But in having that location, I use
17 the example of www.law.pitt.edu, do obtain the content of
18 that information. It is that crossing of the line I think
19 that there is concern about.

20 Now, certainly on-line pornography is a clear
21 problem on the internet but you used the phrase 12
22 percent, at least 88 percent of internet content that is
23 not pornography, that people go out and seek. People use
24 the internet now for everything. Things that they sought
25 by phone, by letter, that they didn't bother to get at all

1 they use the internet. So they are using the internet to
2 obtain information.

3 The First Amendment to the Constitution and
4 this is an area that as a librarian where I might wear my
5 other hat I'm very concerned about. People have the right
6 to access information and that does include the right to
7 access information that some people might find offensive
8 or even obscene although I will be absolutely clear that
9 does not include a right to find, to access child
10 pornography as it is defined under both state and federal
11 law. The line is absolute and is not crossable.

12 Because of the ability to use the internet to
13 find all of this information, legislation or any action
14 that allows government authority, again I feel like I'm
15 sort of standing, you know, against government, and I'm
16 absolutely not. But the government authority is where the
17 Fourth Amendment is invoked, the government authority
18 whether through prosecutors, police agents or others has
19 to obtain search warrants for that kind of information
20 protected by privacy.

21 The view that I have essentially is that
22 network address information, the IP address. Now the
23 scenario that Mr. Freed presented of having that
24 information provided to him as a tip and trying to verify
25 who has that information again, I don't think that that

1 crosses that constitutional, that first, that Fourth
2 Amendment line. But I have to say the second scenario
3 that he presented with the travelers, that starts to cross
4 into content information. He indicated you are talking
5 about the contents of the exchange between the two people.
6 Certainly that content in his hypothetical was absolutely
7 egregious and absolutely should be investigated and
8 prosecuted to the fullest extent. But it does cross the
9 line into content information.

10 And that's where I do get a little bit
11 troubled. If there is a mechanism in place in order to
12 prevent the crossing of that line on the strength of an
13 administrative subpoena alone, then I don't have concerns
14 about this. But if there is no mechanism to prevent the
15 obtaining of content information whether guilty or
16 innocent but content information, then I think the
17 Constitution, Fourth Amendment does require a search
18 warrant or at least some form of court interactions.

19 There are mechanisms within the Electronic
20 Communications Privacy Act for court review and court
21 approval of something slightly short of a search warrant.
22 Search warrants solves all the problems. It doesn't, once
23 you have a search warrant there is the no longer a
24 constitutional or privacy related issue.

25 To be clear, the law is still somewhat

1 unsettled on this. I located a 2008 decision that
2 indicated that IP addresses were not protected by privacy,
3 could be obtained. That is the limit of what we are
4 talking about here. The court did note in a footnote that
5 they recognize the difference between IP address and URL,
6 the web address.

7 And while they did not go to the web address,
8 they used the phrase they felt it was Constitutionally
9 problematic. I guess my concern is that if there is no
10 mechanism to prevent the crossing of that line of, from
11 seeking information, excuse me, from seeking content
12 envelope information to seeking content information, then
13 if content information is sought, whether deliberately or
14 obtained otherwise, then you could run into fruit of the
15 poisonous tree problems wherein all subsequent information
16 is problematic. I would hate to see that happen.

17 I respect completely what Mr. Freed said about
18 the workload and the need to have a speeded up process.
19 But when he closed by saying it takes about a day, you
20 know, is a that too much time to spend to make sure that
21 not only are all parties' constitutional rights protected,
22 particularly the innocent party, the party who is not
23 determined to be engaged in this activity, but also to
24 ensure that all subsequent investigation of the individual
25 does not run into any kind of exclusionary problem.

1 I did have a final comment, I did have some
2 concerns just I describe this as a lesser issue. The
3 language provides that if no case or proceeding arises
4 from the production of these materials that it would be
5 returned on written request of the service provider. I
6 would like to see something a little bit stronger to
7 assure that the information is, when determined that it is
8 no longer necessary, appropriate to retain that
9 information it is affirmatively destroyed or otherwise
10 discarded.

11 That concludes my prepared remarks. I will be
12 glad to take questions.

13 CHAIRMAN MARSICO: Questions? Representative
14 Saccone.

15 REPRESENTATIVE SACCONE: Thank you so much. I
16 really do love to hear all sides of this, no one is
17 perfect and we want to hear all perspectives on this kind
18 of thing. I have taken your concerns into consideration.
19 I'm thinking I have a couple questions myself though.

20 You know we talked about the 88 percent versus
21 the 12 percent, obviously you want to protect the
22 innocent. This bill doesn't apply to the 88 percent, it
23 applies to only those that are being investigated for
24 child sexual abuse, not for the person whose internet
25 activity is out there and it is just a casual internet or

1 whatever personal internet, it doesn't really apply to
2 them, it only applies to those we have reason to believe
3 is engaged in some type of child exploitation.

4 You used the example of Pitt law URL
5 information. I say okay, in one sense I understand what
6 you are saying that the IP address could lead to an
7 understanding or finding out their actual web page address
8 and that would lead to content. But their URL, web page
9 address, they have already put out there to be seen. So
10 it is not like it is a secret they are trying to hide
11 content of it.

12 They put it out there for other child
13 pornographers to come in and take a look. So there should
14 be no expectation of privacy because they publishing it
15 for people to take a look at it. I'm having trouble
16 following that concern if you could clarify that a little
17 bit.

18 MR. PIKE: I appreciate that.

19 REPRESENTATIVE SACCONI: The third thing is
20 look, as I understand it, even if a service provider would
21 receive one of these subpoenas and they felt strongly they
22 didn't want to comply for whatever reason, they don't have
23 to comply. They can ask the court, go back to the court
24 and get an actual search warrant, get a court ruling on
25 this. So there is another protection in there to prevent

1 the abuse of using an administrative subpoena to go after
2 content information. So if you have any comment on that,
3 I would be happy to hear it.

4 MR. PIKE: Regarding the first comment, the IP
5 address identifies only the web host, only the server. It
6 does not identify the specific content within the server.
7 An IP address might be assigned to Pitt.EDU, it doesn't
8 necessarily take you to the sub page within Pitt.EDU where
9 the content specifically lies. So there is a distinction
10 between URL and IP address.

11 A couple scenarios here that I think are
12 important. This bill would, would it identify my IP
13 address? The IP address of the computer that the John Doe
14 target is using.

15 And then what, again in the first scenario
16 Mr. Freed talked about, to the extent that that computer
17 has already been identified, simply trying to find out who
18 owns that IP address, there is no constitutional problem
19 there.

20 I guess my concern is more in looking forward.
21 Once that IP, once you know John Doe's IP address and as
22 the phrase you used may be relevant, but it also may not
23 be relevant, John Doe may be engaged in perfectly innocent
24 activity.

25 John Doe may not be engaged in perfectly

1 innocent activity. It is the looking forward that I think
2 my concern is a little bit higher. After I submitted my
3 written testimony I talked to several people that have IP
4 backgrounds far superior than I and asked them if they
5 could with somebody's IP address seek out and find their
6 forward looking activities. And I got three different
7 answers from three different people which I think is
8 pretty typical of the IT Department.

9 But enough to raise again that concern about
10 what kind of forward looking material. Now your other
11 question, sir, using, if the internet service provider
12 declines to answer the administrative subpoena they can go
13 to court. Yes, there is that as a back up. But that
14 still doesn't reach the level of a search warrant which is
15 what is required when you cross that constitutional line
16 from material people have a reasonable expectation of
17 privacy and material that they don't have a reasonable
18 expectation of privacy.

19 So, I think that is helpful. I think that is a
20 step in the right direction. I'm not certain that that
21 step goes far enough to completely resolve any rights
22 issues.

23 REPRESENTATIVE SACCONI: I would just like to
24 add the Fourth Amendment is very clear and I'm a strong
25 advocate of the Fourth Amendment and the right of people

1 to be secure in houses, papers and effects as you said
2 from unreasonable search and seizure shall not be
3 violated. Papers and effects, your address is not your
4 papers and effects. Your papers and effects is get into
5 the content, now you are into papers and effects and I
6 think that is what the Founders were speaking to.

7 And we don't go there with this, we are
8 strictly talking about identifying data here. That is why
9 I'm having trouble to make the leap that you are making
10 with this.

11 I appreciate your comments.

12 MR. PIKE: I would have to go back and
13 double-check my notes but I do believe there are court
14 cases that have found that type of identifying subscriber
15 information, person that identifies any information,
16 identifies a person is included within the concept of
17 papers and effects.

18 REPRESENTATIVE SACCONI: Thank you.

19 MR. KANE: One quick question on the issue of
20 URL versus the IP address, the federal statute limits the
21 information that can be gotten by an administrative
22 subpoena to a temporarily assigned network address. And
23 this bill mirrors that.

24 MR. PIKE: It does.

25 MR. KANE: Does that make a distinction in your

1 mind between URL and --

2 MR. PIKE: I thought long and hard about that.
3 I certainly saw the way the Stored Communications Act
4 addressed, you have to talk more information from internet
5 service provider experts on that. My understanding is
6 that internet addresses, IP addresses can either be
7 permanently assigned or dynamically assigned, dynamic
8 being a temporary internet address.

9 Again to the extent that the IP address that
10 the utility of that is limited to the kind of envelope
11 information kind of verifying that this computer that has
12 already been identified is owned by John Doe. Then I
13 don't think there is that problem.

14 And if you are talking about again the scenario
15 that Mr. Freed referred to, he has a tip, he knows this IP
16 address accesses this information at this particular point
17 in time. And to identify the subscriber associated with
18 that IP address at that particular point in time I think
19 is part of that envelope information that doesn't cross
20 constitutional lines.

21 A permanently assigned IP address that is also
22 the same IP address moving forward that could be used to
23 find out additional information to find out content
24 information, find out Websites being visited, find out
25 chats being engaged in, finding out e-mail being

1 communicated back and forth utilizing that permanently
2 assigned IP address therein you are getting a lot closer
3 to the content line in the sand.

4 MR. KANE: It could be used to lead a path to
5 that, but the subpoena couldn't be used to get that. In
6 other words, you would use that, you would use what you
7 got on the subpoena to build probable cause to get that
8 information, isn't that correct?

9 MR. PIKE: Once you have the IP address, then
10 to me the question, I don't have a clear answer to this
11 question as it is more of a technical question than legal
12 or privacy question, is what further information can you
13 obtain beyond the subscriber connection that you are
14 seeking, what further information can you obtain by reason
15 of having that IP address. AND to the extent that that
16 further information invokes content information, on
17 further investigation by IT specialists within the State
18 Police, within the, you know, community police. Look what
19 happened at Pitt this past spring with the bomb threats.
20 All we had was IP information, we kept digging and
21 digging. It wasn't us, it was the FBI and Secret Service
22 and Homeland Security, we are very pleased they found the
23 person that did that.

24 CHAIRMAN MARSICO: Thank you very much for your
25 time and information. I appreciate it, professor.

1 MR. PIKE: Thank you very much. Next on the
2 agenda is our Major Marshall Martin and Corporal John
3 O'Neil for the Pennsylvania State Police. Welcome. You
4 may proceed.

5 MAJOR MARTIN: Good morning Chairman Marsico,
6 members of the House Judiciary Committee I am Major
7 Marshall Martin, Director of the Pennsylvania State
8 Police, Legislative Affairs Office. With me today is the
9 supervisor of the Computer Crimes Unit, Corporal John
10 O'Neil. On behalf of the Pennsylvania State Police, thank
11 you for the opportunity to present testimony regarding the
12 proposed amendment to Title 18 concerning administrative
13 subpoenas.

14 Currently Pennsylvania law is required to seek
15 Court Orders pursuant to Section 5743 of Title 18 simply
16 to obtain basic subscriber information for any
17 investigation where an internet protocol address is
18 identified. This basic subscriber information includes
19 name, address, user name and other similar information
20 maintained by internet service providers.

21 The legal process which investigators must
22 follow to secure this necessary, albeit basic information
23 is very time-consuming. In most counties with in
24 Pennsylvania when investigators seek to obtain internet
25 provider records they must prepare a written application

1 for a Court Order and a supporting affidavit containing
2 the facts associated with their investigation to the
3 county's District Attorney's office for review. This
4 paperwork can be voluminous and time intensive. After the
5 application and supporting documents are reviewed by the
6 District Attorney's office they are submitted to a Common
7 Pleas Court for approval. In some counties this process
8 requires the investigator to appear before the reviewing
9 judge.

10 Upon approval the Court Order is forwarded to
11 the applicable internet service provider. Depending on
12 the county and its established procedures this process can
13 take up to a week to accomplish.

14 This outdated and untimely process required to
15 obtain basic subscriber information delays law enforcement
16 in its handling of internet related child endangerment
17 investigations. This lengthy procedure presently required
18 of investigators impedes their ability to rapidly identify
19 jurisdiction subscriber information. This has a direct
20 and negative impact on investigations involving the abuse
21 and exploitation of children.

22 These protracted time periods can be
23 dramatically reduced by the use of administrative
24 subpoenas as proposed in House Bill 2590 sponsored by
25 Representative Saccone.

1 The Pennsylvania Internet Crimes Against
2 Children, the ICAC task force which includes members of
3 the Pennsylvania State Police Computer Crimes Unit also
4 handles all cyber tip complaints forwarded from the
5 National Center for Missing and Exploited Children and
6 other sources. Investigations are awaiting assignment to
7 task force members across the Commonwealth.

8 One of the biggest challenges faced by the
9 tasks force is the prompt identification of the proper
10 jurisdictions where criminal offenses have and are
11 presently occurring. Tips typically provide only general
12 location of the crime. The delay associated with the
13 concurrent requirement with the current requirement for
14 Court Orders only serves to exacerbate the problem.

15 House Bill 2590 simply enables Pennsylvania law
16 enforcement personnel to use methods already employed at
17 the federal level and in several other states. With the
18 increasing number of investigations handled by law
19 enforcement, we need to find ways to shorten the time it
20 takes to resolve these important cases. Legislation that
21 enables the use of administrative subpoenas would serve as
22 a means to that end.

23 In conclusion, on behalf of the members of the
24 men and women of the Pennsylvania State Police, thank you
25 for your support and the opportunity to testify before

1 this committee today. And we will be happy to answer any
2 questions that you may have.

3 CHAIRMAN MARSICO: Questions? Representative
4 Ellis.

5 REPRESENTATIVE ELLIS: Marshall.

6 MAJOR MARTIN: Sir.

7 REPRESENTATIVE ELLIS: In your testimony you
8 talk about the task force handling cyber tip complaints,
9 about how many tips do you get a year?

10 CORPORAL O'NEIL: I can't answer that that is
11 actually monitored and distributed through the ICAC, I'm
12 not sure if the Representative may be able to answer that.

13 REPRESENTATIVE ELLIS: Fair enough. I'm just
14 trying to understand the process behind it. You get a
15 cyber tip through this organization. Then you reach out
16 to the local barracks whatever you get a detective and
17 then they have to figure out maybe it is in like my area,
18 maybe it is in Butler Township who has their own police
19 force, maybe it is in Summit Township, Oakland Township,
20 all Butler, Pennsylvania but it is different townships.
21 Then you have to go through that process of finding out,
22 you know, who should be investigating it and then at that
23 point you have to go to the District Attorney. And I can
24 see that would be a typical example that I just gave of
25 what you guys face?

1 CORPORAL O'NEIL: Yes, and actually what you
2 are describing there also causes us issues often some of
3 the peripheral information in the complaint will identify
4 a person or an address that may be inaccurate. So it may
5 be forwarded to Butler and once we identify the IP address
6 and who the subscriber is it may be actually in
7 Philadelphia, so we spent the time to forward to that
8 investigator and we have to re-forward across the state or
9 even out of the state and it has to be reassigned
10 investigative.

11 REPRESENTATIVE ELLIS: Certainly within
12 Pennsylvania there are multiple townships and
13 municipalities with the same name. I know there are two
14 Butler Townships in Pennsylvania. So I can see where that
15 would be.

16 Now, at this point I mean essentially what we
17 are trying to do with this bill is, my understanding is
18 get you a starting address. You are saying that if we can
19 provide a starting address, we save you a week, sometimes
20 ten days.

21 CORPORAL O'NEIL: Yes, sir.

22 REPRESENTATIVE ELLIS: Are there any other
23 instances outside of the cyber stuff where you are
24 utilizing the administrative subpoenas and saving time,
25 can you think of any?

1 CORPORAL O'NEIL: We are not actually using, we
2 don't have access to administrative subpoenas.

3 REPRESENTATIVE ELLIS: In any kind of crime at
4 all?

5 CORPORAL O'NEIL: We do not, not on the police
6 level.

7 REPRESENTATIVE ELLIS: Thank you very much.

8 CHAIRMAN MARSICO: Representative Saccone.

9 REPRESENTATIVE SACCONE: Yes, thank you for
10 your testimony Major Martin. Corporal O'Neil, you are the
11 technical expert. I'm trying to get a handle on some of
12 the technical issues Professor Pike alluded to. Having
13 access to an IP not only helps law enforcement, but how,
14 you know, how it may cross over the line and provide you
15 access to content information or -- can you address that
16 at all a little, technically? Can you explain the IP
17 where that takes you technically when you have an IP
18 address?

19 CORPORAL O'NEIL: The internet protocol address
20 is information that we actually already have that
21 information.

22 CHAIRMAN MARSICO: Can you speak up a little
23 bit?

24 CORPORAL O'NEIL: The internet protocol
25 address, we already have that information. There are no

1 examples that I'm aware of that we would be able to
2 forward, examine anything for content or anything beyond
3 what we are talking about with that basic information.

4 You are not getting the content of some one's
5 e-mail. You are not getting the web pages, not seeing
6 that information. This is simply to identify name,
7 address, basic information we need just to start an
8 investigation.

9 REPRESENTATIVE SACCONI: Thank you.

10 CHAIRMAN MARSICO: Any questions? Well thank
11 you very much for your time and your testimony today. We
12 appreciate seeing both of you again. Thanks for coming
13 out from Harrisburg.

14 MAJOR MARTIN: Thank you for having us.

15 CHAIRMAN MARSICO: Next on the agenda is A.
16 Sheldon Kovach, Senior Deputy District Attorney at
17 Delaware County DA's office. Thanks for the long trip out
18 here that you had.

19 MR. KOVACH: It's been longer. About an \$80
20 taxi ride for me.

21 Good morning ladies and gentlemen, it is my
22 pleasure to be here. My name is Sheldon Kovach, I'm a
23 senior Deputy District Attorney in Delaware County. I.

24 CHAIRMAN MARSICO: For those out west here,
25 where is Delaware County?

1 MR. KOVACH: Delaware County is, and I grew up
2 in Hershey so I know where you are Mr. Chairman. Delaware
3 County is immediately to the west and actually south of
4 Philadelphia. It abuts West Philadelphia. Actually
5 Philadelphia International Airport is in Delaware County,
6 a good part of it which we benefit somewhat from because
7 cargo city is in Delaware County and when contraband comes
8 in we get some benefit from seizures, forfeiture money.

9 But when the airport is expanding it also
10 expands into Delaware County.

11 Ladies and gentlemen, I have been a District
12 Attorney for in excess of 31 years. I'm presently serving
13 as a supervisor in the Special Victims Unit as well as
14 chief of our Law Appeals Unit.

15 I'm the project coordinator for the federally
16 funded Pennsylvania Internet Crimes Against Children Task
17 Force which is housed in the Delaware County District
18 Attorney's office Criminal Investigation Division.

19 In 1999 when Patrick Meehan was our District
20 Attorney, we applied for and we were notified we had been
21 selected as one of ten task force applications that were
22 going to get United States Department of Justice task
23 force grant funding.

24 At that time there were 20 task forces when
25 that second round of task forces was awarded. The

1 Pennsylvania Internet Crimes Against Tack Force is now
2 part of a nationwide network of 61 task forces which
3 covers the nation providing a seamless web of law
4 enforcement coverage comprised of a cooperative group of
5 agencies both local, state, federal, regional and
6 international levels.

7 The Internet Crimes Against Task Force mission
8 is to safeguard children from being victimized by
9 conducting proactive and reactive investigations by
10 diligently working to apprehend and successfully prosecute
11 perpetrators of child abuse.

12 Another important component of the Internet
13 Crimes Against Task Force is educating parents, teachers,
14 children about internet safety, providing training and the
15 necessary equipment for internet crimes against children
16 investigations to members of law enforcement across the
17 Commonwealth. Increasing overall investigative and
18 forensic capacity is an ongoing goal of the Internet
19 Crimes Against Children Task Force program.

20 In addition to attempting to increase the
21 expertise and the numbers of investigators and forensic
22 analysts in this task force, we in essence act as a
23 conduit for the federal funding which we get to residents
24 of the Commonwealth of Pennsylvania.

25 Today the Pennsylvania Internet Crimes Against

1 Task Force has grown to over 90 collaborating affiliate
2 agencies and well over 185 dedicated investigators and
3 prosecutors participating full-time in the battle against
4 on-line child victimization and child pornography.

5 Advances in computer technology and ready
6 availability on consumer level as well as the decline in
7 cost has enabled individuals who are inclined to exploit
8 children, a remarkably effective and far-reaching ability
9 to carry out their criminal activities.

10 These activities include collecting,
11 manufacturing and distributing child pornography and
12 soliciting minors through live chats and streaming videos
13 on demand. The worldwide web knows no boundaries, poses
14 unique and difficult challenges to law enforcement in
15 their efforts to try to protect children from illegal and
16 harmful activity.

17 Child pornographers, pedophiles and other types
18 of child sexual abusers flock to the internet to share
19 information to make contact with children. Child sex
20 offenders are major contributors to children chat rooms
21 frequently pretending to be children themselves.

22 Some pedophiles go farther and actively arrange
23 meetings with children often going to extraordinary
24 efforts, incurring large travel and incidental expenses
25 just to meet a child.

1 Some of these individuals sadly succeed in
2 endeavors. On-line child, sexual exploitation involves
3 three primary activities. The first would be the on-line
4 exchange of child pornography. Next would be arrangements
5 between adults, hard as it may seem, hard to believe those
6 who seek access to children and contact other adults who
7 are willing to provide or trade children for sexual
8 purposes.

9 And thirdly, adults seeking sexual contact with
10 children by establishing friendships with children
11 on-line. Upon having befriended a child on-line the
12 pedophile may then attempt to arrange a face-to-face
13 meeting and ultimately engage in sexual abuse and
14 exploitation of the child. A child's innocence can never
15 be replaced. When a minor has been photographed or
16 videotaped and placed on the internet there will always be
17 a permanent recurring record of the crime each time the
18 child pornography is viewed, downloaded or shared.

19 Children who are involved or exposed to child
20 pornography can become desensitized and socialized into
21 believing that their activity is normal. There are also
22 many children who are totally unaware that they have been
23 recorded and their activities have subsequently been
24 distributed over the internet.

25 Child sexual abuse claims more than one million

1 victims worldwide on an annual basis. Children who have
2 been sexually abused or involved in the production of
3 child pornography demonstrate a multitude of psychological
4 symptoms evidenced by emotional withdrawal, antisocial
5 behavior, wild mood swings, sever depression and
6 unwarranted fear and anxiety.

7 Untreated, victims of child sexual abuse are at
8 high risk to later engage in destructive behavior and to
9 forever carry the misplaced burdens of guilt and shame.
10 When a child is sexually exploited by an adult for any
11 reason, the child is always the victim. Computer
12 technology and the internet make it easier for offenders
13 to exploit children. They allow offenders to arrange
14 meetings with children for sex easily manufacture and
15 distribute child pornography.

16 Offenders are also using the internet to share
17 information about the most effective ways to meet children
18 and locate and groom victims to evade law enforcement
19 detection. As even more children use the internet, police
20 and prosecutors lack sufficient time and resources to
21 effectively investigate and successfully prosecute each
22 and every potential case.

23 Prolific sex offenders who often use the
24 internet to gain access to children must be high priority
25 for law enforcement because they do represent a

1 significant threat to a large number of children.

2 There is a federal prison study that compared
3 incarcerated federal inmates who then were questioned
4 about the number of contacts that they actually had with
5 victims. Surprisingly the prisoners who were in who
6 actually been put in prison for sexual contact, direct
7 sexual contact with a child reported fewer victims when
8 they were given free rein to self report, be honest than
9 those who were in federal prison who were doing time for
10 child exploitation via possession of child pornography or
11 attempting to lure children over the internet.

12 The range of victims for the one category where
13 there was actual contact were serving prison sentences was
14 from zero to 40. The range of victims for the child
15 pornographers via the internet was zero to over 200.

16 Computer technology and the internet make it
17 easier for offenders to exploit children, allows offenders
18 to arrange meetings with children for sex, to easily
19 manufacture, distribute child pornography.

20 The internet allows offenders to circumvent
21 many of the traditional safeguards which we as parents,
22 community have in place to protect children. An internet
23 offender can communicate with a number of potential
24 victims simultaneously across the country or worldwide.

25 The problem continues to grow as technology

1 becomes more affordable and more children access the
2 internet through mobile wireless high speed technologies.

3 The United States Department of Commerce
4 through a study shows internet use is increasing
5 regardless of income, education, race or gender and
6 children and teenagers use computers and the internet more
7 than any other group.

8 Among the different kinds of internet child
9 sexual abuse child pornography clearly ranks as the
10 highest in sheer numbers of cases that need to be
11 investigated. Sexual predators and possessors of child
12 pornography enjoy seeming anonymity on the internet and
13 can lurk in chat rooms and search for the next child
14 victim to satisfy their desire for child pornography,
15 sexual encounters, obtaining a list or any of the above
16 combined.

17 The Pennsylvania Internet Crimes Against Child,
18 Children Task Force annually receives well over 2,000
19 documented complaints of computer facilitated child sexual
20 exploitation.

21 I just glanced at the semiannual reports, we
22 had closer to 3,000 over the course of a year, six months
23 there was 1600 tips, and another six months there was 1500
24 tips.

25 The Internet Crimes Against Children Task Force

1 has apprehended over 2500 offenders, submitted over 75
2 cases of child sexual exploitation to the National Center
3 for Missing and Exploited Children Child Victim
4 Identification program. In addition, the Pennsylvania
5 Internet Crimes Against Children Task Force identified
6 more than 50 victims of child exploitation or sexual abuse
7 across Pennsylvania.

8 The Pennsylvania ICAC task force has
9 significantly improved the capability and number of law
10 enforcement prosecutors, forensic examiners and analysts
11 with expertise in investigating child exploitation.
12 However, given the sheer number of cyber tips distributed
13 by the National Center which must be processed, analyzed
14 and forwarded to the appropriate municipal jurisdiction
15 for further investigation in a timely manner along with
16 recently developed and highly refined computer software
17 programs which make for virtually limitless number of
18 possession and distribution of child pornography cases
19 which could be investigated, there are simply many more
20 cases of child pornography and sexual exploitation that
21 can be investigated than time and resources will allow.

22 At present the Internet Crimes Against Children
23 investigator will identify and computer source for which
24 there are specific a computer source for which there are
25 specific and articulable facts that demonstrate that there

1 are reasonable grounds to believe that a search of the
2 computer's content will yield relevant and material
3 evidence of ongoing criminal that activity.

4 In order to obtain a name and address or
5 network subscriber information for the subject computer, a
6 Grand Jury subpoena or judicial process must be utilized.
7 No matter how routine it may become, of course, the police
8 investigators have these petitions and proposed orders on
9 the computer. It nevertheless is still a time-consuming
10 endeavor. Preparing a search warrant or a petition and
11 proposed Court Order and finding and getting approval of a
12 judge needlessly consumes a chunk of time which could be
13 more effectively used to pursue more case investigations
14 resulting in the apprehension of more individuals who
15 victimize children.

16 The existing option of using a Grand Jury
17 subpoena is not practical in most counties because the
18 majority of the counties in the Commonwealth do not
19 impanel investigative Grand Juries. The convening of an
20 investigating Grand Jury in addition to being a costly
21 process really is only justified when all other avenues of
22 investigation have been exhausted and when without the
23 powers and resources of a Grand Jury the criminal activity
24 cannot be fully investigated.

25 Depending on whether an investigation

1 originates from the National Center via a cyber tip or
2 from one of the law enforcement Websites and information
3 survey systems determines how many Court Orders are needed
4 before a search warrant for content based information can
5 be obtained.

6 A simple case may require obtaining both a
7 Court Order for internet service provider information and
8 then a second court order to the ISP to obtain an address
9 and billing information relevant to the time of the
10 suspected criminal conduct.

11 A review of Pennsylvania's Wiretap Electronic
12 Surveillance Act shows that the act already provides for
13 the use of administrative subpoena authorized by statute
14 to procure non-content information. What House Bill 2590
15 does is it becomes a substantive enabling provision needed
16 to implement the administrative subpoena process that had
17 already been in the statute.

18 House Bill 2590 tracks the federal language
19 found in the Stored Wired and Electronic Communications
20 Act. Under existing United States Supreme Court precedent
21 an individual has no Fourth Amendment privacy expectation
22 in most records that are maintained by third parties.

23 Now Pennsylvania jurisprudence differs in
24 construing Article I Section 8 of the state's Constitution
25 largely because they focus a heavier focus on invasion of

1 privacy issues. However, the 2003 case of Commonwealth
2 versus Duncan which was decided by our Pennsylvania
3 Supreme Court held that a person does not have a
4 reasonable expectation of privacy in his name and address
5 and that prevent police from obtaining such information
6 from their banking records associated with an ATM card.

7 In that case, it was a rape case. The ATM card
8 the police simply made a call to the bank and the bank
9 disclosed the name and address of the user of the ATM card
10 which led to the ultimate prosecution and conviction of
11 the rape defendant and the Supreme Court did not find that
12 to have any constitutional problem.

13 The Pennsylvania Supreme Court's lengthy
14 discussion of the realities of modern day society and the
15 applicable two-prong inquiry regarding a person's
16 subjective expectation of privacy and whether the
17 expectation objectively is one that society recognizes as
18 reasonable and legitimate I believe would negate any
19 serious constitutional challenge to obtain non-content
20 based information which discloses nothing about one's
21 personal or private affairs.

22 An investigation relating to sexual
23 exploitation or abuse of children time is of the essence.
24 With limited resources and the astronomical number of
25 leads which must be pursued House Bill 2590 would better

1 enable law enforcement to more effectively and efficiently
2 follow up leads and allow for more cases to be
3 investigated in the same amount of time.

4 Protecting children from the harm of the
5 creation, possession and distribution of child pornography
6 and direct contact sexual victimization is clearly of
7 paramount importance to everyone. Serving one more or
8 saving one more child victim from a lifetime of misery
9 makes this legislative effort worthy of expeditious
10 consideration.

11 I thank you and your committee in drafting the
12 legislation. It was one of two priorities that we had
13 written in on our Internet Crimes Task Force
14 administrative subpoenas, we were hoping to get
15 legislation and also concern about the long arm statute
16 which I think is or will be discussed.

17 So I appreciate your efforts and one addition,
18 it is not just the possession of child pornography. One
19 of the reasons that we feel pressure in processing these
20 tips is because there are children who can be sexually
21 abused as a result of the investigation. And when one
22 looks at the delay and says gee, had we not gone through
23 this cumbersome process it would be a month earlier than
24 we would have gotten to that child. We would submit there
25 is nothing that is of a constitutional dimension which

1 should keep this committee from approving this bill.

2 CHAIRMAN MARSICO: Thank you very much. I
3 guess it was a year or two ago that we did tour your
4 facility, your unit in Delaware County. And we had a very
5 important information meeting about this issue. And, in
6 fact, your unit director, I can't think of his name --

7 MR. KOVACH: Lieutenant Peiffer, Task Force
8 Commander.

9 CHAIRMAN MARSICO: Yes, actually we did have
10 discussion about this particular piece of legislation,
11 this idea. I just was really impressed by the way the
12 unit operates.

13 Interaction with other DAs and the state police
14 and AG's office, how do you, walk us through that
15 interaction partnership.

16 MR. KOVACH: We have presently in Delaware
17 County the DA office, we have two forensic, we have two
18 analysts and the cyber tips I mentioned which come in
19 maybe 15 to 20 a day these analysts process those cyber
20 tips. When they process them, of course a lot of them
21 they will dismiss because they are 1-800 hot line calls to
22 the National Center, they then geographically will send
23 them to the respective task forces.

24 If there is potential criminal activity, the
25 analyst then makes up a file. He gets the right

1 municipality or jurisdiction to investigate. There are
2 over 90, I think about 27 counties. There is a lot of
3 municipal police agencies involved in the internet crimes,
4 of course, the State Police can cover the entire
5 Commonwealth. They are then farmed out to the proper
6 locality.

7 But we initially or they initially would have
8 to get a Court Order to identify this internet service
9 provider. And then whose computer. It is amazing in
10 addition to the cyber tips I mentioned the refined
11 sophisticated system. You can look on a map at anyone
12 time thanks to the State Police and their work with called
13 operation round-up, at any one time can look at the
14 Commonwealth of Pennsylvania and see who is sharing child
15 pornography.

16 So then it is a matter of prioritizing. That
17 is not cyber tips, that is independent of cyber tips,
18 prioritizing who is sharing child pornography, what is the
19 number, who is sharing the largest number. At that point
20 then prioritize who you are going to investigate.

21 Depending on the municipality they either get a
22 search warrant or petition and Court Order from the judge
23 to ultimately identify the location, the name, the billing
24 address, where that comes back. Ultimately then
25 content-based information after that one or two set of

1 Court Orders if there is probable cause to do a search of
2 the computer, wherever it is located at, a search warrant
3 must be obtained which of course would be judicial review.
4 Upon determination of probable cause detectives or police
5 will go in and do a search. We still don't know who the
6 perpetrator is, if it is possessing child pornography.

7 We know it comes from that particular computer
8 but many times you go into the household and you know it
9 is not the grandmother paying the bill or the father, but
10 it might be a 25-year-old, 30-year-old son who is living
11 with them.

12 So you are still not identifying personal
13 information by knowing the billing information for the
14 computer as to who actually had downloaded this
15 pornography, or who was communicating with the child.

16 CHAIRMAN MARSICO: Thank you. Representative
17 Ellis, questions?

18 REPRESENTATIVE ELLIS: Thank you CHAIRMAN
19 MARSICO just a couple questions. You pointed to the one
20 study about self reporting. If I'm reading this right, I
21 think this is what you said, the person who commits the
22 act of exploiting a child, if they do it for lack of
23 better terms the old fashion way through meeting the
24 child, luring them in for whatever purposes, does it that
25 way, they are less likely to have contact than somebody

1 who uses the internet as their means?

2 MR. KOVACH: In average number of victims. To
3 be candid, that study was because it was a federal prison
4 study, the other side would say well, the child
5 pornographers who were doing time in federal prison were,
6 the possessors of the worst child pornography or the
7 largest numbers. But from the standpoint of through
8 polygraphing and really didn't have anything to lose when
9 they were truthful, they ultimately actually had more
10 contact sex offenses than the offenders who were in the
11 federal prison study who were in prison for actually
12 having contact.

13 REPRESENTATIVE ELLIS: It is very alarming. If
14 you think about there may have been one person in, you
15 know, in a community that was trying to do this. Now that
16 same person can be doing it anywhere in the United States,
17 get on a plane for 129, 150 bucks fly somewhere to make
18 contact and, you know. Certainly the work you guys do is
19 amazing.

20 If there was a way that we could help speed
21 that process, I think we have to continue to look at ideas
22 like this.

23 MR. KOVACH: We really appreciate that. It is
24 amazing to us the internet traveler cases where we have
25 undercover detectives in a sting to, it is amazing they

1 come as far as California to Delaware County just to meet
2 a child. They have driven as far as Indiana, Ohio,
3 Illinois to meet a child.

4 Those cases actually take a lot more time to
5 investigate as opposed to the child pornography possession
6 cases.

7 REPRESENTATIVE ELLIS: If I can just ask going
8 in a slightly different direction, I have been working
9 with the committee for a while now on human trafficking
10 legislation, obviously there are children being exploited
11 across the Commonwealth too. Is that something that your
12 task force is also mindful of and, you know, certainly do
13 we see internet usages in human trafficking now?

14 MR. KOVACH: Actually the last two years was
15 written into our grant. We have one particular Assistant
16 District Attorney who is very interested, and I think she
17 is on the Governor's Commission as well, a woman by the
18 name of Pearl Kim.

19 So that is written in as well. Yes, the state
20 trafficking statute, we obtained the first conviction in
21 Delaware County under that statute. It is very generally
22 worded. It was a conviction that resulted as a result of
23 for lack of a better term a pimp who among his victims
24 that he prostituted out was a teenager through an
25 undercover detective he met this teenager and ultimately

1 obtained a conviction of that person who had procured her
2 and arranged for this meeting.

3 So that is, absolutely one of the priorities
4 written in. Also it is a priority of the U.S. Department
5 of Justice.

6 REPRESENTATIVE ELLIS: Thank you for everything
7 you do.

8 CHAIRMAN MARSICO: Thank you Representative
9 Saccone, questions?

10 REPRESENTATIVE SACCONE: Yes, thank you,
11 question/comment. I'm an old investigator from the
12 Department of Defense. You know, investigations included
13 these type of cases our military duty civilian stationed
14 military mail, so forth we look at these things and I
15 would say dealing with some of the perpetrators of this,
16 would you agree that the guile of these people knows no
17 bounds and they are, they are capable of luring young
18 people in and they take, they're very patient and take
19 time to lure multiple victims at once especially on the
20 internet working on several victims at a time until they
21 place them, this one is further along, I will get this one
22 first, this one I'm working long-term, so forth. It seems
23 to have know no bounds.

24 Time is of the essence is my point. Any time
25 we can save getting these people, save children that might

1 be touched by these deranged people who are preying on our
2 children, would agree with that?

3 MR. KOVACH: Absolutely. And in addition to
4 the guile they have, that success for the vulnerable child
5 who they meet with, speak in the internet they have that
6 knack as to who is the most vulnerable.

7 REPRESENTATIVE SACCONI: My other question,
8 maybe that would be better meant for the technical expert,
9 if we pass this legislation, I think it will be a
10 successful step forward. Are we missing anything, about
11 you know, because these guys are clever, will they now
12 look at some other way to conceal their identity, should
13 we have been addressing some other part of this that we
14 failed to prevent, forward looking to prevent them from
15 circumventing what we are going to pass hopefully to help
16 find them, help law enforcement find them, are we missing
17 anything that might help us, some visionary thing that
18 might help us prevent them from circumventing the law in
19 the future?

20 MR. KOVACH: I have to plead, I am a legal
21 person, but not, I'm kind of a dinosaur when it comes to
22 computer technology. In reading the statute it certainly
23 satisfied the primary purpose. But you are correct,
24 Representative Sacconi, we never can quite keep up with
25 what is developing on the other side but we've attempted

1 to do that. The long arm statute business is another
2 issue which we are fortunate that when we send a Court
3 Order to California, it is honored.

4 But a long arm statute that would authorize
5 that would be a better way to do it.

6 REPRESENTATIVE SACCONI: Thank you.

7 CHAIRMAN MARSICO: Thank you very much for the
8 hard work that you do, the work you do for the
9 Commonwealth. Just once again thank your unit, and
10 Lieutenant Peiffer?

11 MR. KOVACH: Yes.

12 CHAIRMAN MARSICO: Thank him for his help as
13 well.

14 MR. KOVACH: We appreciate your efforts.

15 CHAIRMAN MARSICO: I want to thank Jefferson
16 Borough for having us here today and also want to announce
17 that the committee will consider this bill next Tuesday,
18 September 25th, if that is the correct date. So once
19 again I thank all the testifiers for being here today.

20 I thank Representative Saccone for his
21 leadership with this bill and the members that are here
22 and staff. This concludes our hearing and once again
23 thanks everyone for being here and for your hospitality in
24 the Borough of Jefferson, thanks.

25 (Adjourned at 11:30 p.m.)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CERTIFICATE

I, William E. Weber, RDR, CRR do hereby certify that the
above testimony is a true and correct copy of said
proceedings.

William E. Weber, RDR, CRR