Bonnie Seaman. It's hard to think of any work I have done these past ten years without Bonnie. Another theme of this book is loyalty, and few people have taught me more about the trait than Bonnie. I am deeply indebted to her for the skill and good spirit she brings to our work right up to this day.

That was written more than 20 years ago—just about 22 years ago. Of course, I can say the same thing about Bonnie's work in the U.S. Senate. In 1996, when I was elected the State's auditor general, Bonnie was vital to, first, my transition team. Then she served as the director of the Office of the Auditor General for 8 years, where she oversaw day-to-day operations of my schedule and the management of staff. When I was elected State treasurer in 2004, Bonnie began work with the Treasury Department. Then, finally, when I was elected in 2006 to the Senate, I asked Bonnie to serve as director of constituent services. I knew that her dedication to public service and compassion for others would make her an excellent director. She led the office of constituent services for 10 years with distinction. With her gold standard professionalism, and unimpeachable ethics, she was a mentor to her staff and served as a shining example of quality public service. Through her work, Bonnie has touched the lives of over 60,000 Pennsylvania constituents.

On behalf of my family, as well as thousands of families across our Commonwealth, I express our gratitude to Bonnie Seaman for more than three decades of stellar public service. The building we worked in, in Harrisburg, has this inscription on the front of it, the finance building: ''All public service is a trust, given in faith and accepted in honor.'' Bonnie accepted the trust that was placed in her. She kept faith with taxpayers and brought honor to her work. I wish Bonnie well in her retirement as she travels with her husband Tom, attends yoga classes, and enjoys time with her family and friends.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Arkansas.

(The remarks of Mr. COTTON pertaining to the introduction of S. 1202 are printed in today's RECORD under ''Statements on Introduced Bills and Joint Resolutions.'')

Mr. COTTON. I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. STRANGE). The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. UDALL. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

## RECESS

The PRESIDING OFFICER. Under the previous order, the Senate stands in recess until 2:15 p.m.

Thereupon, the Senate, at 12:31 p.m., recessed until 2:15 p.m. and reassembled when called to order by the Presiding Officer (Mr. PORTMAN).

## EXECUTIVE CALENDAR—Continued

The PRESIDING OFFICER. The President pro tempore, the Senator from Utah.

### INTERNATIONAL DATA PRIVACY

Mr. HATCH. Mr. President, I rise today to discuss international data privacy. This is a critically important issue that has become all the more important over the years as we become more sophisticated. It has become all the more pressing in recent months as a result of court decisions impacting law enforcement's ability to access electronic communications overseas.

I don't think it would surprise anyone to hear me say that our privacy laws have not kept pace with technological developments. The primary statute that governs law enforcement's ability to access electronic data, the Electronic Communications Privacy Act, or ECPA, was enacted over 30 years ago—long before most people had even heard of email or the internet. ECPA was drafted in a world in which electronic data was stored on personal computers or on servers located in offices or homes. It presumes a world where data is in one location and where in order to access data, a person simply goes to the relevant location and retrieves it. But that is not the world we live in, at least not today. Nowadays, much of our data is stored not on home or office computers but in the cloud, a network of remote servers spread throughout the world that allows us to access data from literally anywhere.

The rise of cloud and remote network computing has transformed the way companies and individuals store data. No longer is data stored on sites or in one discrete location; rather, data pertaining to a single individual or even to a single document may be stored at multiple sites, spread across countries or even across continents. This has created all sorts of complications for our laws.

ECPA requires law enforcement to obtain a warrant before it can access many types of electronic communications. It also prohibits disclosure to foreign entities. Warrants, however, traditionally have stopped at the water's edge. A judge here in Washington can issue a warrant authorizing law enforcement to search an office here in Washington but cannot issue a warrant for searches in London or Paris.

So what is law enforcement to do in a world of cloud computing where pieces of the same electronic document might be stored in Washington, London, and Paris?

One possibility is to say that as long as the data is accessible from the United States—that is, so long as you can retrieve it by logging on to a computer somewhere in the United States—that is all that matters; law enforcement can order its disclosure.

This sort of maximalist approach, however, brings with it a whole host of problems. To begin with, it pays scant attention to the laws and interests of other countries, including our closest allies. Other countries, it turns out, have data privacy laws of their own, and just like ECPA, sometimes these laws prohibit disclosure to foreign entities, including foreign law enforcement. So to say U.S. law enforcement can compel disclosure and data stored anywhere in the world so long as that data is accessible in the United States is really to say that U.S. law enforcement can override the laws of other countries.

More particularly, it is to say U.S. law enforcement can order individuals or companies that store data overseas to violate the privacy laws of other countries. This is unfair to service providers who may find themselves on the wrong side of the law no matter which side they choose and does little to help international relations. It also undermines trust, drives customers to foreign competitors, and undermines the privacy of U.S. citizens by emboldening other countries with less robust privacy regimes that similarly seek unlimited extra territorial access to data.

Another possibility is to say that if the data is stored in the United States, then law enforcement may access it, but if it is stored outside our borders, it is off limits.

This is essentially the current state of affairs following a decision last summer by the U.S. Court of Appeals for the Second Circuit that ECPA warrants do not reach data stored abroad. Under the Second Circuit's decision, U.S. law enforcement can use compulsory process to access data stored in the United States but must work through diplomatic channels to obtain data stored overseas.

This sort of domestic storage regime has the benefit of avoiding the conflict-of-laws problems I have just described, but it also has very real drawbacks.

To begin with, it impedes law enforcement's ability to solve and prevent crime in cases where the needed data is stored outside the United States, even when the creator of the data is an American, the service provider storing the data is an American, and the crime being investigated took place here in the United States. The mere happenstance that the data is stored beyond our borders, even though it may constantly or instantly be accessed from within our borders, places it off limits. Service providers' varying business practices in moving and holding data determine whether an investigation moves forward.

This sort of domestic storage regime also forces U.S. law enforcement to work through diplomatic channels, which sometimes are slow and sometimes very cumbersome and in many instances less protective of privacy than U.S. criminal process, which requires a warrant from a neutral magistrate and a finding of probable cause.